Albertina Maria Duarte

Segurança Informática

O caso das escolas secundárias da cidade da Praia

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

5.10.11

Albertina Maria Duarte

Segurança Informática

O caso das escolas secundárias da cidade da Praia

Universidade Jean Piaget de Cabo Verde

Campus Universitário da Cidade da Praia
Caixa Postal 775, Palmarejo Grande
Cidade da Praia, Santiago
Cabo Verde

5.10.11

Albertina Maria Duarte, autora da monografia intitulada *Segurança Informática: o caso das escolas secundárias da cidade da Praia*, declaro que, salvo fontes devidamente citadas e referidas, o presente documento é fruto do meu trabalho pessoal, individual e original.

Cidade da Praia aos 30 de Setembro de 2011
Albertina Maria Duarte

Memória Monográfica apresentada à Universidade Jean Piaget de Cabo Verde como parte dos requisitos para a obtenção do grau de Licenciatura em Informática de Gestão.

Sumário

Este trabalho monográfico, intitulado *Segurança Informática: o caso das escolas secundárias da cidade da Praia*, tem como objectivo principal compreender os principais conceitos e técnicas de segurança e auditoria informática e conhecer a realidade da segurança informática nas escolas secundárias da cidade da Praia, analisando as práticas da segurança informática nas mesmas. Para este estudo recorreu-se a uma metodologia baseada por um lado, na pesquisa qualitativa e por outro, numa abordagem quantitativa.

No quadro da pesquisa qualitativa, utilizou-se a pesquisa bibliográfica, que serviu de suporte para debruçar sobre os aspectos da segurança e auditoria informática que constituem a base deste trabalho. A segurança informática pode ser resumida num conjunto de medidas que possibilita a um sistema informático garantir os princípios de autenticidade, disponibilidade, integridade e disponibilidade. Por seu lado, a auditoria permite verificar se tais medidas são práticas de segurança no sistema informático e se as mesmas estão em conformidade com as regras e procedimentos existentes na política de segurança de uma organização.

Na abordagem quantitativa, onde foi realizada parte prática, os resultados indicam que nenhuma das escolas em estudo, dispõem de uma política de segurança. Foi nesse sentido que sugeriu-se como proposta de melhoramento a criação de um documento formal que especifica as regras, normas e princípios de segurança informática, bem como as respectivas sanções, ou seja, uma política de segurança para as escolas secundárias da cidade da Praia.

Agradecimentos

Este trabalho foi concretizado graças à colaboração de várias pessoas que directa ou indirectamente deram algum contributo para que tal acontecesse, por isso, manifesta-se gratidão a todas essas pessoas, mas considera-se pertinente particularizar as seguintes:

- A minha família a qual devo tudo o que hoje tenho e sou.
- O meu professor e orientador, Isaías Barreto da Rosa, pela disponibilidade e conselhos sempre sábios e oportunos.
- A todos os meus colegas, que foram não só companheiros, mas acima de tudo amigos durante esses cinco anos de crescimento e de amadurecimento.

Conteúdo

Tabelas

Gráficos

Abreviaturas

ACL – Access Control List

CA – Certification Authority

CobiT – Control Objectives for Information and Related Technology

DES – Data Encryption Standard

DMZ – DeMilitarized Zone

GRE – Generic Routing Protocol

HIDS – Host-based Intrusion Detection Systems

ICMP – Internet Control Message Protocol

Il TEC – Instituto de Linguística Teórico e Computacional

IETF – Internet Engineering Task Force

IDS – Intrusion Detection Systems

IP – Internet Protocol

IPSEC – IP Security

ISO – International Standards Organization

ISACA – Information Systems Audit and Control Foundation

L2F – Layer 2 Forwarding

L2TP – Layer 2 Tunnelling Protocol

NIDS – Network-based Intrusion Detection Systems

OSI – Open System Interconnection

PPTP – Point-to-Point Tunnelling Protocol

RSA – Rivest Shamir Adleman

RAID – Redundant Array of Independent Disck

TCP – Transmission Control Protocol

TI – Tecnologias de Informação

TIC – Tecnologias de Informação e Comunicação

UDP – User Datagram Protocol

UPS - Uninterruptible Power Supply

URL – Uniform Resource Locator

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

Introdução

1.1 Enquadramento

A segurança é uma necessidade de qualquer ser humano, ou seja, o homem como um ser dependente que é por natureza, para se sobreviver necessita de vários cuidados, entre eles está a segurança/protecção. Transportando isso para o mundo das tecnologias pode-se dizer que todo o recurso/informação possui o seu valor e, por isso, precisa ser protegido contra os diferentes tipos de ataques.

A preocupação com a segurança informática não é recente, segundo Mamede (2006) ela existiu desde o inicio da utilização de meios automáticos para o tratamento e armazenamento da informação, sendo essa segurança inicialmente relacionada apenas com questões de disponibilidade e protecção do meio ambiente. Silva (2005) vai mais longe e fala de escritos codificados em tempos em que ainda se escreviam em pedras de argila, mais tarde, durante a segunda guerra mundial utilizaram algoritmos de codificação para evitar que informações confidenciais fossem lidas por inimigos. O mesmo autor (*idem*) afirma que para além do sigilo da informação, começaram a preocupar com a segurança do equipamento devido ao seu grande custo, além da segurança com o ambiente físico, essa preocupação era posteriormente estendida a formas de recuperar os dados em caso de ocorrência de algum dano por acidente ou avaria em algum equipamento, surgindo assim as cópias de segurança.

Quando começaram a utilizar ambientes de computação em redes e consequentemente com o surgimento da internet[1], os problemas de segurança aumentaram-se brutalmente, pois passou a existir a possibilidade da propagação, em pouco espaço de tempo, de aplicações com conteúdo malicioso como, por exemplo, a contaminação por vírus, além disso, passou a existir ainda a possibilidade do acesso remoto não autorizado, ultrapassando todos os limites geográficos e temporais. Zúquete (2008) defende que, o que torna a internet um meio extremamente favorável ao surgimento de ataques é o anonimato e o facto deste interligar um conjunto descontrolado de redes.

Na verdade, ao analisar a sociedade actual, pode-se notar que os problemas de segurança continuam a aumentar, juntamente com os rápidos avanços tecnológicos, o que exige uma postura pró-activa por parte das organizações baseada em atitudes simples mas, que podem trazer ganhos significativos, como por exemplo, manter o sistema actualizado.

A passagem da sociedade industrial para a sociedade de informação que se vive hoje, faz com que as TI assumem um papel cada vez mais preponderante no desenvolvimento das organizações, consequentemente a pertinência de garantir a segurança informática aumenta paralelamente a essa dependência das tecnologias. Nesta linha de pensamento, pode-se então dizer que a segurança deve ser um pré-requisito e encarada como um factor prioritário e essencial para o sucesso dos negócios, para as organizações que buscam vantagem competitiva. Contudo, a estratégia de implementação da segurança numa organização deve ser bem definida, por forma a estabelecer um equilíbrio entre os custos e os benefícios.

As escolas secundárias como organizações estão inseridas nessa tal sociedade de informação pois, a qualidade de ensino passa por investir em TI, como forma de se ter acesso a informações sempre disponíveis e actualizadas. Assiste-se hoje a uma preocupação no sentido de apetrechar as escolas com as TI, mas pouco se tem falado sobre a segurança informática nas escolas secundárias. Daí surge o interesse pelo tema: *segurança Informática: o caso das escolas secundárias da cidade da Praia.*

[1] "A Internet é uma extensa rede de computadores interligados, mas independentes", Heide Stilborne (2000) citado por Silva (2005)

1.2 Justificação da escolha do tema

Este trabalho para além das razões de ordem intelectual, isto é, aumentar o conhecimento na área de informática, prima-se também para satisfazer as razões de ordem prática, pois pretende-se apresentar algumas contribuições a nível da definição de medidas de segurança que podem servir para a melhoria da segurança informática das escolas em estudo.

1.3 Objectivos do trabalho

1.3.1 Objectivo geral:

- Compreender os principais conceitos e técnicas de segurança e auditoria informática e conhecer a realidade da segurança informática nas escolas secundárias da cidade Praia, analisando as práticas da segurança informática nas mesmas.

Para facilitar a compreensão do objectivo geral, entendeu-se decompô-los nos seguintes objectivos específicos.

1.3.2 Objectivos específicos:

- identificar as vulnerabilidades existentes no sistema informático;
- identificar as medidas e políticas de segurança existentes e praticadas nas escolas;
- certificar/averiguar da sensibilidade dos responsáveis pelo sistema informático pelas questões de segurança;
- propor, a partir dos resultados obtidos, melhorias para a segurança informática nas escolas secundárias.

Como pode-se reparar, os objectivos supracitados exigem uma escolha cuidada de métodos, técnicas e procedimentos, isto é, uma metodologia à natureza do estudo.

1.4 Metodologia

Se é verdade que a busca de informações fundamentadas para a realização deste trabalho levou-se a reconhecer a necessidade de uma escolha cuidada de instrumentos de recolha de informação, não é menos verdade afirmar que associado, quer aos instrumentos, quer aos métodos e técnicas de recolha de dados está a decisão pela escolha, tanto da pesquisa qualitativa como pela pesquisa quantitativa.

No quadro da pesquisa qualitativa[2], utiliza-se a *pesquisa bibliográfica*, tendo em conta a necessidade de se ter como suporte contribuições teóricas tecidas por alguns autores que já debruçaram os seus estudos sobre a temática em apreço e/ou outros assuntos afins.

Na abordagem quantitativa[3], utiliza-se o *método estatístico*, no tratamento dos dados, seguindo as seguintes etapas:

i. Escolha da amostra, pois num universo de 10 escolas secundárias subdivididas pela cidade da Praia, optou-se por uma amostra de 80%.

ii. De seguida elaborou-se um conjunto de aspectos sobre segurança informática, aos quais quis-se verificar da sua existência junto dos responsáveis das instituições em estudo, recorrendo a *aplicação de uma checklist*.

iii. Por fim, fez-se o *tratamento estatístico dos dados*, através do programa SPSS versão 15.

1.5 Estrutura do trabalho

A par da introdução e conclusão, este trabalho apresenta na sua estrutura três capítulos: no Capítulo 1 que tem por título segurança informática nas organizações, apresenta-se as

[2] A abordagem qualitativa é voltada para a descoberta, a identificação, a descrição aprofundada e geração das explicações, como dá-nos conta Michel (2005).
[3] Michel (2005) define a abordagem quantitativa como sendo aquela em que toda a actividade de pesquisa se recorre à quantificação, quer no momento de recolha de informação, quer no tratamento destas.

contribuições de alguns autores sobre este tema, nomeadamente a definição de segurança informática sem esquecer as propriedades de segurança, os níveis da segurança informática, ou seja, segurança a nível físico, lógico e de recursos humanos e, ainda refere-se a política e planos de segurança; no Capítulo 2 incide-se sobre a auditoria informática, básicamente este capítulo consistiu em definir a auditoria infomática e referir aos diferentes testes que podem ser feitos aquando da realização de uma auditoria, refere-se ainda neste capítulo a alguns padrões da auditoria; no Capítulo 3, isto é, o último, foi destinado ao trabalho de campo, pois procura-se verificar *in loco* a aplicação do sistema de segurança informática nas escolas secundárias da cidade da Praia.

Capítulo 1: Segurança informática nas organizações

1 Enquadramento

Este capítulo, objectiva apresentar as referências teóricas pertinentes e, sobretudo, indispensáveis face aos objectivos traçados, permitindo, por conseguinte, estabelecer a ponte com a componente prática que vai-se, mais adiante, desenvolver. Na verdade, nesta parte são apresentadas as contribuições tecidas por alguns autores que têm debruçado sobre a segurança informática que, assume-se como linhas de orientação desta investigação.

Foi com este propósito que procurou-se começar por apresentar o conceito da segurança informática na perspectiva de alguns autores, igualmente, outros pontos são aqui desenvolvidos nomeadamente as propriedades, objectivos da segurança informática, a segurança física, lógica, e de recursos humanos, políticas e planos de segurança.

2 Conceito da segurança informática

Segundo o pensamento de Downing *et al* (2001: 513) a segurança informática é "a protecção dos computadores quanto a falsificação e divulgação indesejável de dados".

De acordo com Simões (2004) “a segurança de um sistema informático pode ser entendida como um conjunto de medidas que visam a protecção desse sistema contra ameaças que afectem a confidencialidade, integridade e disponibilidade da informação processada”.

Para Mamede (2006: 10) a segurança informática é “ (…) prevenção e detecção de acções não autorizadas por utilizadores de um sistema de computadores”.

Oliveira (2000: 13) afirma que a segurança é “ (…) a restrição dos recursos de um microcomputador, ou de uma rede, ou de porções desta rede para outros utilizadores ou computadores. Segurança não é mais do que a gestão de tal restrição (…)”.

A segurança dos sistemas de informação se define, de acordo com Carneiro (2002: 2) como “ (…) um conjunto de medidas e procedimentos, que têm por finalidade evitar que a informação seja destruída, alterada ou acedida, incidental ou intencionalmente, de uma forma não autorizada”.

Segundo Il Tec (1993) a segurança do sistema informático é um “conjunto de medidas técnicas e administrativas aplicadas a um sistema de processamento de dados para proteger o equipamento, o suporte lógico e os dados contra modificações, destruição ou divulgação, quer acidental quer intencional”.

Partindo dos conceitos acima apresentados, pode-se perfeitamente, concluir que todos têm a sua razão de ser, contudo o conceito apresentado por Simões (2004) é para nós, o mais pertinente, pois entende-se que para se proteger os recursos das TI da organização é necessário ter já definido um conjunto de medidas com base numa análise dos riscos, ou seja, identificar todas as vulnerabilidades e ameaças e consequentemente as formas de ultrapassá-las antes de serem exploradas pelos atacantes. A segurança informática implica ter capacidade de antecipar ou, pelo menos, minimizar ocorrências indesejadas ou acções não autorizadas, garantindo que os sistemas sejam confiáveis, íntegros e disponíveis.

Existem alguns requisitos a que um sistema informático deve atender quando se fala em segurança informática, que são as propriedades de segurança, propriedades essas que de seguida passa-se a desenvolver.

3 Propriedades de segurança

Qualquer organização, independentemente da área em que ela opera, ela lida com informações de algum valor e daí a necessidade de serem protegidas. Devido ao facto de grande parte das informações serem acedidas com recurso à internet, estão sujeitas a vários tipos de ameaças desde a simples escuta de uma mensagem, até à alteração do seu conteúdo.

Monteiro e Boavida (2000: 312) afirmam que "o problema da segurança em sistemas e redes pode ser decomposto em vários aspectos distintos, dos quais são, (…) reconhecidos como mais relevantes os seguintes: autenticação, confidencialidade, integridade, controlo de acesso, não repudiação e disponibilidade". São essas propriedades básicas de segurança que garantem uma circulação mais segura das informações dentro de uma organização ou entre organizações, as quais de seguida se apresenta.

3.1 Autenticidade

Monteiro e Boavida (2000: 312) definem a autenticidade como " (…) o processo através do qual é validada a identidade de um utilizador, dispositivo ou processo". Por outras palavras, a autenticação significa garantir que o emissor da mensagem é realmente que se diz ser, garantir a correcta identidade como medida de protecção da informação. A autenticação previne alguns tipos de ataques como a personificação (a personificação acontece quando uma entidade tenta passar por outra, e pode acontecer por parte de quem envia ou de quem recebe a mensagem) e o não repudio (quando o legítimo autor de um acto nega a sua execução por simples arrependimento ou por má fé). De acordo com Medeiros (2001) o serviço de autenticação pode ser implementado por mecanismos de *password* ou assinatura digital, os quais debruça-se nos próximos pontos deste capítulo.

3.2 Confidencialidade

Segundo Mamede (2006: 80) "por confidencialidade entende-se o manter seguro o conteúdo de uma mensagem evitando que possa ser acedido por alguém não autorizado para o fazer, tornando-se dessa forma conhecedor do mesmo". Esta propriedade garante o acesso a

informações apenas a utilizadores autorizados, evitando desta forma a intercepção (acessos não autorizados sem contudo alterar o envio ou o conteúdo de uma mensagem) de mensagens. A confidencialidade é particularmente importante para empresas em que a sua vantagem competitiva assenta nas informações que estas detêm.

3.3 Integridade

Como afirma Mamede (*idem*: 80) a integridade pode ser entendida como " (…) a detecção de alterações como sejam adições ao conteúdo, eliminação parcial ou qualquer outra modificação por pessoas não autorizadas a fazê-lo". Como pode-se entender, a integridade permite evitar a modificação de mensagens por utilizadores sem permissão para tal, ou seja, garante que um documento autêntico não foi alterado acidental ou intencionalmente.

P.Silva *et al* (2003) afirmam que qualquer que seja a modificação ou erro que ocorra sobre os dados originais, a mensagem deixa de ser íntegra, podendo comprometer um enorme volume de dados, acarretando elevados prejuízos.

3.4 Controlo de acesso

O controlo de acesso é um outro objectivo de segurança informática e garante que aos recursos de um sistema só sejam acedidos apenas por utilizadores com autorização para o fazer. Mais detalhes sobre este aspecto serão descritos noutros pontos deste capítulo.

3.5 Disponibilidade

Monteiro e Boavida (2000: 312) defendem que "os aspectos de disponibilidade garantem que, mesmo após a ocorrência de ataques a uma dada rede ou sistema informático, os recursos chave ficam disponíveis para os utilizadores". A disponibilidade, neste caso, refere-se à continuidade de serviços, para tal há que criar sistemas que garantem a redundância de serviços. De nada vale ter a informação necessária, mas não a ter disponível no momento, por isso, deverá haver um equilíbrio entre a necessidade de acesso e as medidas utilizadas na protecção de acesso às informações.

Diante da grande quantidade de ameaças a que um sistema informático está sujeito, deve existir uma preocupação no sentido de garantir as principais propriedades de segurança acima citadas. Quando se pretende proteger um conjunto de dados/informações, há que se levar em conta a segurança, considerando três aspectos: segurança física, segurança lógica e segurança de recursos humanos, os quais de seguida passa-se a desenvolver.

4 Segurança física

Steinke (2002) citado por Mamede (2006: 259) afirma que "a segurança física pode ser definida como o conjunto de medidas que podem ser tomadas para garantir a segurança e existência de algo ou alguém contra roubo, espionagem, sabotagem ou qualquer dano". Como o próprio nome indica, essas medidas têm por objectivo garantir a segurança dos recursos a nível físico.

O mesmo autor (*idem*: *ibidem*), acrescenta que "o principal papel da segurança física é manter as pessoas não autorizadas ou não desejadas fora das instalações e do acesso a bens da organização e garantir o comportamento dos colaboradores como especificado nas regras". O mesmo é dizer que se devem criar os mecanismos de segurança que impeçam por um lado, as pessoas não autorizadas ter acesso a instalações e, por outro, criar restrições de acesso dentro da organização a locais onde estão alojados equipamentos que contenham informações críticas para a organização.

Quando se fala em proteger os recursos a nível físico deve-se levar em conta vários tipos de ameaças que de acordo com Carneiro (2002) as principais são:

- desastres naturais, incêndios acidentais, trovoadas e inundações;
- ameaças ocasionadas por elementos humanos;
- distúrbios, sabotagens internas e externas deliberadas.

Para evitar tais ameaças e garantir a segurança física devem ser considerados vários aspectos entre os quais: localização geográfica das instalações; controlo de acesso; segurança do equipamento, que de seguida se apresentam.

4.1 Localização geográfica das instalações

Um dos primeiros aspectos a ter em conta no que se refere à segurança física, diz respeito à localização de um centro de informática e da vulnerabilidade a que este pode apresentar perante diferentes ocorrências indesejadas.

Neste sentido P.Silva *et al* (2003), propõem algumas medidas de segurança a nível da localização dos centros de processamento de dados tais como:

- um centro de informática não deve ficar localizado nem no primeiro piso, nem no último, se se tratar de um edifício térreo, deverá fazer o possível para afastar o centro de processamento de dados das vias de circulação, bem como das condutas de águas ou de esgotos;
- os acessos a esses centros deverão ser facilmente monitorizados e não deverão existir quaisquer acessos directos para o exterior, mas devem dispor de saídas de emergência;
- o chão e o tecto das instalações devem ser falsos para permitir a passagem das condutas necessárias à alimentação energética e processamento de atmosfera (conduta e saída para ar condicionado);
- os sistemas de alimentação eléctrica devem ser redundantes;
- deverão existir sistemas de detecção e combate a incêndios apropriados.

Estes requisitos de localização dos centros de processamentos de dados destinam-se a garantir um bom nível de segurança, contudo o que acontece muitas vezes é que empresas são instaladas em edifícios já existentes e com estrutura própria. Nestes casos devem ser feitos os ajustes necessários para minimizar ou evitar o máximo possível as consequências de acidentes naturais ou acidentes de origem humana.

4.2 Controlo de acesso

Para além dos cuidados a ter com a localização geográfica, deverão ser criados mecanismos de segurança que permitem acesso apenas a pessoas autorizadas às áreas dos recursos das TI. O nível de protecção deve variar de acordo com o grau da segurança dos dados que se pretende proteger.

A restrição de acesso físico deve ser definida tanto para as pessoas externas à organização, como para as pessoas internas, que são as detentoras do sistema de informação e por isso as mais difíceis de controlar, pois existem áreas consideradas sensíveis, nomeadamente a sala de servidores, que não podem ser acedidos de igual modo para todos os colaboradores da organização. Para Mamede (2006: 69) "os controlos de acesso físico destinam-se a limitar o acesso físico directo a hardware, a dispositivos de armazenamento de informação, à intra-estrutura física da rede, a registos escritos de senhas, entre muitos outros itens"

Ferreira e Alves (1995) apontam algumas formas de controlo de acesso físico nomeadamente: recorrer a dispositivos de controlo de acesso personalizados que dão detalhes sobre a entrada e saída das instalações (sistemas de vídeo-vigilância, uso de cartões magnéticos, sistemas biométricos); nas áreas de segurança, todo o pessoal deve dispor de formas de identificação; os direitos de acesso devem ser cessados assim que a pessoa abandone a organização.

P.Silva *et al* (2003) defendem que os registos de acesso, particularmente a zonas sensíveis, deverão ser verificados pelos responsáveis de segurança para que as questões duvidosas possam ser esclarecidas em tempo oportuno.

4.3 Segurança do equipamento

O ambiente das organizações caracteriza-se por uma dependência cada vez maior dos equipamentos informáticos pois, neles circula todo o fluxo de dados/informações indispensáveis para o funcionamento de uma organização. Torna-se assim, importante definir um conjunto de procedimentos que permitem manter os recursos informáticos em segurança, particularmente os equipamentos que suportam actividades críticas.

Para Ferreira e Alves (1995), os equipamentos devem estar protegidos dos perigos ambientais e das oportunidades de acesso não autorizadas. Para isso estes autores destacam os seguintes tipos de protecção:

- protecção global dos edifícios e dos locais: a arquitectura, a estrutura, os materiais de construção dos locais onde estão implantados os equipamentos devem ser pensados levando em conta a garantia de segurança;

- protecção global do meio envolvente: estabelecer medidas de protecção contra poluição química e radiações electromagnéticas;

- protecção contra intrusões físicas externas: medidas de controlos de acesso físico, protecção contra incêndio (equipamentos informáticos devem estar localizados em locais distantes de combustíveis e inflamáveis, também, devem ser instalados e vistoriados regularmente equipamentos como detectores de calor e de fumo, alarmes contra incêndios, extintores de incêndios e devem existir saídas de emergência); protecção contra inundações; protecção da instalação eléctrica (dispor os equipamentos críticos de sistemas UPS); protecção do nível de climatização (a temperatura não deve ultrapassar os 18ºC e a humidade não deve estar acima de 65%), medidas anti-intrusão (alarmes, sistemas de vídeo-vigilância);

- protecção contra intrusões físicas internas: controlo da circulação das pessoas; vedação e blindagem dos compartimentos; recursos básicos como os bastidores devem ser localizados fora de acesso público.

Além de todas essas formas de protecção dos equipamentos informáticos Carneiro (2002) acrescenta que estes devem ser periodicamente sujeitos a uma verificação técnica e monitorizado o seu estado de conservação e de limpeza.

Todos estes mecanismos de defesa do controlo de acesso físico, permitem evitar o arrombamento físico, ou seja, evitar este tipo de ataque que acontece quando há acesso físico não autorizado ao departamento dos recursos das TI, podendo atentar à integridade física das máquinas. Do mesmo modo que se preocupa em garantir a segurança física, os dados/informações também devem estar protegidos, daí a importância da segurança lógica.

5 Segurança lógica

A segurança lógica segundo Carneiro (2002) refere-se à segurança da utilização do *software*; protecção dos dados, dos processos e dos programas; acesso autorizado dos utilizadores. Isso mostra que sem a segurança lógica, toda a informação de uma organização fica exposta aos vários tipos de ataques, e que, por isso, deverá ser criado um conjunto de medidas que impede o acesso indevido a informações, seja local ou remotamente. Para garantir a segurança lógica, Mamede (2006) destaca vários aspectos a serem levados em consideração nomeadamente: autenticação e controlo de acesso; *firewall*; detecção de intrusões; antivírus; filtragem de conteúdos; criptografia; assinaturas digitais; certificados digitais; redes locais virtuais; redes privadas virtuais, os quais passa-se a fazer referência.

5.1 Autenticação e controlo de acesso

P.Silva *et al* (2003: 80) afirmam que a autenticação e o controlo de acesso "são quem assegura que nós somos quem dizemos ser e que nos permite aceder àquilo a que temos direito, quer a nível da infra-estrutura (redes de comunicações), quer a nível aplicacional, através do fornecimento de credenciais do nosso conhecimento exclusivo". A autenticação neste caso, garante que apenas os utilizadores autorizados tenham acesso aos recursos disponibilizados, o que constitui portanto, a base para o controlo de acesso aos recursos.

Os controlos de acesso lógico têm por objectivo segundo Mamede (2006: 70) " (…) limitar o acesso a dispositivos como, por exemplo, impressoras, bem como a outros recursos e serviços, como sejam informação, aplicações e sistema, e ainda funcionalidades diversas". Por sua vez, Monteiro e Boavida (2000: 328) afirmam que "as funções de autenticação estabelecem a identidade de utilizadores e/ou sistemas, tendo em vista a determinação das acções permitidas". Através da identificação do utilizador, se possibilita o processo de autenticação, onde se verifica se o utilizador é realmente quem se diz ser, ou seja, a autenticação permite verificar a identidade de um utilizador. A identidade de um utilizador e a sua autenticação estabelecem as permissões e as restrições aos diversos recursos da organização a que este está sujeito.

A autenticação da identidade do utilizador pode ser implementada de quatro formas, conforme diz Carneiro (2002):

- aquilo que se conhece, o utilizador possui um segredo, e que por isso, é apenas do conhecimento deste, são exemplos *password*, um número de identificação pessoal, etc.;

- aquilo que se possui, o utilizador é detentor de algo que mais ninguém tem, por exemplo um cartão magnético;

- aquilo que se é, consiste em sistemas capazes de medir características físicas únicas de cada pessoa, como por exemplo, a utilização de sistemas de biometria, através de reconhecimento da voz, reconhecimento facial, impressão da retina, impressão digital;

- leitura de um elemento que o utilizador é capaz de fazer (os padrões de escrita, assinatura digital).

A autenticação, ainda pode ser garantida com base num sistema híbrido, ou seja, na combinação de mais do que um dos mecanismos acima descritos, dependendo dos recursos financeiros e do nível de segurança que cada empresa pretende implementar.

Monteiro e Boavida (2000) defendem que a autenticação por *password* é um dos mecanismos mais utilizados, devido sobretudo à sua simplicidade e ao seu baixo custo em comparação com os outros. Contudo, apresenta frequentes fragilidades, devido muitas vezes à falta de sensibilização dos utilizadores para sua correcta definição e utilização. Isso, exige uma boa gestão dos mesmos, que implica por um lado, sensibilizar os utilizadores para a importância da utilização de *password* seguro e, por outro, implementar medidas que permitem detectar *password* inseguro, antes de serem explorados pelos atacantes.

Cliff (2001) citado por Medeiros (2001) distingue duas técnicas de adivinhação de *password*:

- utilização de dicionários: refere a utilização de programas com dicionários de diversas línguas contendo palavras, frases, letras, números, símbolos, ou qualquer outro tipo de combinação que possa ser utilizada para a combinação de *password*;

- ataque à força bruta: consiste em fazer todas as combinações possíveis de caracteres até conseguir a *password* pretendida. A sua eficácia depende de quão difíceis de adivinhar forem. Este método de descoberta de *password* é mais lenta que a utilização de dicionários.

O controlo de acesso e a autenticação estão directamente relacionados e são usados simultaneamente, já que o perfil de um utilizador é que vai definir as suas permissões e as suas restrições. Um dos mecanismos de controlo de acesso bastante utilizado é o *firewall* que, passa-se de seguida a apresentar.

5.2 Firewall

Se uma organização pode criar as condições para controlar a sua rede interna, mais difícil se torna controlar a rede externa, a internet, por ter um padrão de comunicação aberto, ficando sujeito a vários tipos de ameaças. Assim o *firewall* é um dos dispositivos cujo objectivo é criar formas de segurança para controlar o tráfego entre a rede protegida (interna) e a chamada rede não confiável (rede externa).

Monteiro e Boavida (2000: 354) definem *firewall* como " (…) um equipamento computacional colocado na zona de fronteira de uma rede, cujo principal objectivo é o controlo de acesso a essa rede por parte de utilizadores sediados noutras redes". Como podemos ver pela definição desses autores, *firewall* é um importante mecanismo de segurança, pois permite executar um conjunto de restrições, protegendo uma rede confiável de uma não confiável, ou seja, deixando entrar os pacotes com permissão e bloquear os que não têm permissão.

Para Zúquete (2006) uma *firewall* tem dois objectivos fundamentais:

- protecção por isolamento de máquinas ligadas à rede;
- controlo de interacções entre máquinas.

Quanto às tipologias de *firewall*, Monteiro e Boavida (2000) defendem que existem diferentes tipos de *firewall* que podem ser classificados em três categorias:

- filtro de pacotes;
- *firewalls* de aplicação;
- *firewalls* baseados em estado.

5.2.1 Filtro de pacotes (estáticas)

Segundo Mamede (2006: 272) "os *firewalls* de filtro de pacotes (*packet filtering*) baseiam-se fundamentalmente nos cabeçalhos IP TCP, UDP, ICMP dos pacotes individuais dos diferentes protocolos para permitirem ou negarem o tráfego (…) ". Nesse caso, a decisão sobre o reencaminhamento ou não de um pacote é baseada nas informações encontradas nas camadas de rede (responsável pelo endereçamento de pacotes de rede) e transporte (responsável pela movimentação dos dados) do modelo OSI (modelo de arquitectura de sistemas de comunicação, que serve de base para implementação de qualquer rede). Estas informações incluem o endereço IP origem e destino, a porta origem e destino, e o protocolo. A lista de controlo de acesso (ACL) constitui a base de dados do sistema de *firewall* onde residem as regras, ou os filtros, com base nos quais são analisados os pacotes.

De acordo com o mesmo autor (*idem*) este tipo de *firewall* apresenta alguns inconvenientes: limita-se apenas a filtragem do cabeçalho dos pacotes, sem contudo inspeccionar o conteúdo dos mesmos; acesso directo do sistema externo a qualquer sistema interno, possibilitando aos atacantes o acesso a diferentes portas; é vulnerável a ataques como o *Spoofing*[4]. Em contrapartida, apresenta principais vantagens: o baixo custo, não é necessário equipamento adicional, normalmente baseado em *routers*; rapidez; flexibilidade e transparência, etc.

5.2.2 Ponte aplicacional

Também designado por *proxy server* (*application gateway*), este tipo de *firewall* de acordo com Mamede (2006: 279) "funciona transferindo uma cópia de cada pacote de dados aceite de uma rede para outra, mascarando desta forma a origem dos dados". Deixa de haver a comunicação directa entre cliente e o servidor externo, pois o servidor *proxy* vai actuar como

[4] Spoofing "é a técnica de se fazer passar por outro computador da rede para conseguir acesso a um sistema". Neto e Solonca (2007)

o intermediário entre o cliente e o servidor, garantindo maior segurança na rede interna. Quando o *proxy* recebe os pedidos do exterior, analisa-os de acordo com as condições estabelecidas, reencaminha o pedido ou nega o tráfego, o mesmo acontece quando o pedido tem origem no interior da rede, o *firewall* faz a intercepção da informação e inspecciona-os, podendo ser reencaminhados ou não.

Se por um lado, este tipo de *firewall* apresenta como limitação a exigência de uma maior complexidade de configuração e manutenção, pois requer um *proxy* específico para cada aplicação, por outro, tem vários pontos fortes tais como: actua como repositório temporário de informação (podendo registar todo o tráfego, seja ele de origem interna ou externa; todos os dados pedidos são armazenados no próprio *proxy*) o que traduz num melhor desempenho, uma resposta mais rápida no acesso a internet; não existe o contacto directo entre o servidor remoto com qualquer outro dispositivo dentro da rede interna; funciona na camada da aplicação, permite a autenticação do utilizador e controlo de acesso; Mamede (*idem*).

5.2.3 Filtro de circuito

Os *firewalls* baseados em estados para Monteiro e Boavida (2000: 360) " (…) analisam o tráfego aos níveis IP e TCP/UDP, e constroem tabelas de estado das ligações, de modo a prevenir ataques por *spoofing*, *replaying* e outros. Para além disso possibilitam um funcionamento ao nível de aplicação, também de forma dinâmica". Nesse tipo de *firewall* as decisões de filtragem são tomadas não só com base nas informações dos cabeçalhos, mas também numa tabela de estado, onde estão guardados os estados de todas as conexões. Assim como *firewall* baseado em pacotes, este também trabalha na camada de rede.

5.3 Detecção de intrusões

Os sistemas de detecção de intrusão ou IDS, de acordo com P.Silva *et al* (2003), oferecem visibilidade a uma organização das várias tentativas de intrusão, tanto no que sucede no seu exterior, como no que sucede internamente.

M.Silva *et al* (2003) alegam que muitas vezes é possível fazer passar pelo *firewall* algum tráfego de natureza maliciosa, já que este toma as decisões com base na origem e destino dos

dados e não no seu significado, para isso utilizam-se os sistemas de detecção de intrusão que têm por função procurar anomalias no conteúdo dos dados ou quaisquer indícios de ataques à segurança dos sistemas.

Os mesmos autores (*idem*) dividem os sistemas de detecção de intrusão em dois grandes grupos, a seguir descritos.

- IDS baseados em sistemas, HIDS: são programas dedicados a sistemas individuais que permitem identificar quais processos e utilizadores estão envolvidos em algum tipo de ataque no sistema.

  Bece (2001) citado por Medeiros (2001) descreve algumas vantagens e desvantagens dos HIDS. Como vantagens afirma que podem operar num ambiente onde o tráfego de rede é criptografado; podem ajudar a detectar cavalos de Tróia[5] ou outros tipos de ataques que envolvam problemas de integridade nos programas a nível do sistema operacional. As desvantagens apontadas por este autor são: HIDS são difíceis de se gerir, pois cada *host* monitorado precisa ser configurado; como as informações para análise dos HIDS estão armazenadas no *host*, um atacante pode invadir o sistema e desabilitar essas funcionalidades; este tipo de IDS consome recursos de processamento do *host* monitorado, influenciando a sua performance.

- IDS baseados na rede, NIDS: tem por finalidade monitorar todo o tráfego de rede, ou seja, os ataques são capturados e analisados através de pacotes de rede. Bece (2001) citado por Medeiros (2001) apresenta algumas vantagens e desvantagens deste tipo de IDS. A grande vantagem é que não interfere no funcionamento e desempenho da rede, pois funciona no modo passivo, apenas escutando o tráfego na rede; fica invisível aos atacantes. Contudo, apresenta dificuldade em processar todos os pacotes numa rede com grande tráfego de dados; não pode analisar o tráfego de informações criptografadas; tem problemas em lidar com pacotes fragmentados; etc.

[5] Cavalos de Tróia são “programas de computador com funções destrutivas camufladas, tal como apagar os discos numa data determinada” Downing (2001: 80)

5.4 Antivírus

Nos dias de hoje com a proliferação de técnicas cada vez mais sofisticadas de código malicioso, torna-se uma necessidade de qualquer organização que lida com os recursos das TI, dispor de mecanismos antivírus no seu sistema informático. Downing (2001: 26) define antivírus como "*software* que protege o computador de vírus (modificações destrutivas de *software*), impedindo as modificações que um vírus tente efectuar ou detectando, logo que seja possível um vírus que se introduza no computador".

Amado (2006: 4) acrescenta ainda que um sistema antivírus "inclui as ferramentas e utilitários destinados a proteger o seu computador de ser infectado por programas, vírus e afins indesejados, e que de algum modo podem afectar, em maior ou menor escala, o comportamento do seu computador".

Segundo Mamede (2006: 150) são vários os sinais que podem alertar para a existência de vírus num sistema, nomeadamente:

- o sistema aparenta ter menos memória do que deveria;
- o sistema reinicia sozinho;
- alguns ficheiros ficam corrompidos ou não se comportam como o esperado;
- alguns ficheiros ou programa desaparecem;
- ficheiros ou programas desconhecidos aparecem no sistema;
- mensagens estranhas aparecem no ecrã, entre outros.

As soluções de antivírus podem ser baseadas em assinatura ou em comportamentos. A assinatura segundo P.Silva *et al* (2003: 98) é "um excerto de código binário único de um vírus, que permite a identificação do vírus em questão por um simples processo de comparação". Assinatura procura características binárias identificativas de código malicioso. Por seu lado, o comportamento para os mesmos autores (*idem*: 99) "inspira-se na detecção de intrusões e promete um nível superior de eficácia na detecção e contenção de infecções".

A actualização é igualmente um aspecto fundamental, independentemente das TI que se está a utilizar, o sistema antivírus deve estar configurado para fazer actualização automática. Normalmente os fornecedores de antivírus dispõem de sites que permitem fazer a actualização dos mesmos. P.Silva *et al* (2003), afirmam que existem soluções centralizadas para realizar automática e permanentemente a actualização e a disseminação dessas mesmas actualizações por todos os sistemas que se pretende proteger, a partir de um ponto único. Mamede (2006: 61) acrescenta ainda que "o sistema antivírus deverá estar instalado em cada servidor e em cada computador pessoal e em cada computador pessoal da organização".

5.5 Filtragem de conteúdos

Os mecanismos de filtragem de conteúdos não se limitam em detectar mensagens em que os anexos podem conter algum código malicioso, mas desempenham outras funções especificamente em mensagens de correio electrónico ou conteúdos *Web* e podem ser usados juntamente com o sistema antivírus.

Entre outras funções de filtragem de conteúdos podemos indicar a restrição a determinados acessos em termos de utilização da internet (como, por exemplo, cópia de filmes, acesso a conteúdos pornográficos, etc.); restringir o acesso a *software* ilegal, ou seja, definir o que é permitido e o que é negado aos utilizadores. É igualmente função deste mecanismo detectar e impedir tentativas de transmissão de informação confidencial de acordo com P.Silva *et al* (2003). Tais restrições podem ser feitas, de acordo com os mesmos autores (*idem*) com base nas listas de endereços URL[6], ou com base nas palavras-chave relacionadas com quaisquer temáticas que se pretende bloquear.

M.Silva *et al* (2003: 173) afirmam que muitas organizações " (…) recorrem a esse tipo de serviços para garantir que os seus colaboradores não ocupam o seu tempo de trabalho a aceder a conteúdos que nada tenham a ver com a actividade profissional". Por outras palavras, filtragem de conteúdos, garante às organizações que os seus colaboradores não consomem o seu tempo em actividades que não estão directamente relacionadas com a

[6]URL (*Uniform Resource Locator*) é a forma única e exacta de localizar a informação disponível na internet, Downing (2001)

função que desempenham, o que resulta numa economia para a empresa em termos de recursos gastos para suportar actividades como por exemplo *downloads* ilegais.

5.6 Criptografia

Oliveira (2000: 405) define a criptografia como "um conjunto de técnicas que tornam uma mensagem incompreensível permitindo apenas que o destinatário que conhece a chave de encriptação consiga desencriptar e ler a mensagem com clareza". O objectivo de criptografia, neste caso, é utilizar algoritmos de codificação e descodificação, por forma a que o conteúdo da mensagem só pode ser acedido por utilizadores com autorização para o fazer.

Monteiro e Boavida (2000) distinguem duas categorias básicas de mecanismos de codificação: criptografia simétrica, também chamada de criptografia de chave secreta ou partilhada e criptografia assimétrica ou criptografia de chave pública.

5.6.1 Criptografia simétrica

Na criptografia simétrica é utilizada uma única chave para cifrar e decifrar a mensagem. O emissor codifica a mensagem utilizando um algoritmo conhecido e uma chave secreta e envia, ao receber, o receptor descodifica a mensagem com a mesma chave secreta, conforme afirmam Monteiro e Boavida (2000). Nesse caso, segundo Mamede (2006), se a chave for quebrada num dos extremos toda a mensagem fica comprometida, e muitas vezes o outro extremo pode não se aperceber que a mensagem está comprometida. É recomendável que a mensagem e as chaves sejam transmitidas usando canais de comunicação diferentes.

Este mesmo autor (*idem*) afirma que não obstante a sua velocidade que permite cifrar grandes quantidades de informação, apresenta como principal limitação o problema da gestão das chaves que pode ser desdobrada nos seguintes pontos:

- se a chave é perdida, todo o canal fica comprometido;
- convém mudar frequentemente de chave, para evitar o comprometimento da mesma;

- a distribuição das chaves é crítica, pois se houver algum comprometimento das chaves no momento em que as mesmas são distribuídas, todas as mensagens que utilizarem essas chaves podem ser decifradas por quem o interceptou;

- são necessárias várias chaves, aumentando o risco e a probabilidade da ocorrência de fuga de informação.

Para Mamede (*idem*) um dos algoritmos utilizados na criptografia simétrica é o DES. P.Silva *et al* (2003) afirmam que o DES é utilizado como *standard* para protecção da informação, desde 1981; surge depois o TripleDES ou 3DES, composto por três operações sequenciais de cifra utilizando o DES, ou seja, para proporcionar maior segurança e aumentar o nível de protecção da informação, aplica o DES três vezes, utilizando chaves diferentes.

5.6.2 Criptografia assimétrica

Monteiro e Boavida (2000) afirmam que o processo da criptografia assimétrica funciona utilizando um par de chaves, uma pública que pode ser livremente divulgada e uma privada que é mantida secreta e deve ficar apenas na posse e uso da pessoa ou entidade a que pertence. O emissor cifra a mensagem com a chave pública do receptor, este ao receber a mensagem, ele vai decifrar a mensagem com a sua chave privada.

De acordo com Oliveira (2000) o algoritmo mais conhecido para a criptografia assimétrica é o RSA. Este algoritmo, de acordo com Medeiros (2001) pode ser usado tanto para criptografia de informações como para o sistema de assinatura digital.

Se por um lado, a grande vantagem da criptografia assimétrica segundo Medeiros (2001) é que ultrapassado o problema de gestão das chaves, já não há necessidade de se ter um canal seguro para a transmissão da chave secreta, ou seja, o emissor não tem que dar ao receptor a conhecer secretamente a chave, porque a chave que cifra é diferente da que decifra a informação, tornando o processo mais seguro.

Por outro, Mamede (2006: 87) afirma que “este tipo de criptografia é mais lenta que a criptografia simétrica, exigindo maior poder computacional”. Um outro problema ligado à

utilização da criptografia assimétrica, segundo P.Silva *et al* (2003) é que este tipo de criptografia não garante a autenticidade do remetente, ou seja, se a chave que cifra é a pública que pode ser trocada livremente, não há quaisquer garantias que a chave é a do destinatário pretendido. A autenticação, nesse caso, é garantida com recurso a assinatura digital, que de seguida passa-se a descrever.

5.7 Assinatura digital

Mamede (2006: 88) defende que "uma assinatura digital mais não é do que um código digital anexado a uma mensagem transmitida de forma electrónica e que identifica univocamente o emissor e garante a integridade da mensagem". Ou seja, uma assinatura digital tanto garante que a mensagem não foi alterada, como garante que o remetente é realmente quem diz ser.

O mesmo autor (*idem*) aponta as seguintes propriedades da assinatura digital:

- não-forjamento, significa que quem assinou fê-lo deliberadamente, já que utilizou a sua chave privada para o efeito;
- autenticidade, garante que quem assinou é identificável;
- não-reutilização, garante que a assinatura digital não pode ser reutilizada em outros documentos;
- não-repudiação significa que quem assinou não pode negar que o fez;
- integridade, ou seja, um documento assinado digitalmente não pode ser alterado.

Segundo Mamede (*idem*) uma assinatura digital pode ser feita tanto com base na criptografia simétrica, como na criptografia assimétrica.

Na assinatura digital com base na criptografia simétrica, é necessário a existência de um árbitro que desempenha o papel central de todo o processo e partilha com cada utilizador uma chave secreta. O emissor cifra a mensagem com a chave que partilha com o árbitro e envia-o. Este decifra a mensagem e cifra novamente com a chave que partilha com o receptor e envia ao receptor juntamente com o certificado de validade. Este ao receber a

mensagem, decifra-a com a chave que partilha com o árbitro, podendo ver em anexo o certificado de validade. Como se pode ver nesse tipo de assinatura digital, o árbitro tem de ser uma pessoa de confiança para ambas as partes, para não comprometer todo o processo.

A assinatura digital com base na criptografia assimétrica, de acordo com Mamede (*idem*), funciona da seguinte forma:

- a mensagem a ser enviada é cifrada com a chave pública do receptor;
- simultaneamente, a mensagem é passada pela função de *hash* (comprime grandes quantidades de informação numa sequência de *bits*, protegendo a autenticidade de mensagens) e cifrada com a chave privada do emissor e obtém-se a assinatura digital que é anexada à mensagem e de seguida enviada ao receptor;
- este, por sua vez, decifra a mensagem com a sua chave privada e depois determina o *hash* da mensagem;
- a assinatura digital é decifrada com a chave pública do emissor e obtém o *hash* que foi determinado antes do envio;
- o receptor faz a comparação entre o *hash* da assinatura digital e o *hash* da mensagem. Se esta comparação resultar em valores iguais quer dizer que a mensagem é íntegra e autêntica, ou seja, não houve qualquer alteração à mensagem durante o processo de transmissão da mesma.

A questão que se pode colocar é: como obter de forma segura a chave pública? O ponto que de se seguida desenvolve-se responde a tal questão.

5.8 Certificados digitais

Os certificados digitais permitem ultrapassar o problema existente na assinatura digital, ou seja, como obter de forma segura a chave pública de um determinado utilizador.

Oliveira (2000: 408) afirma que o certificado digital “é o processo de garantir que uma chave pública pertence efectivamente a uma pessoa ou entidade. (…) é garantido pela assinatura

digital de uma pessoa ou entidade confiável, a Autoridade Certificadora (CA)". Pode-se dizer, então que os certificados digitais são ficheiros que contêm a chave pública e as informações pessoais do seu dono, ou seja, associa a identidade do utilizador à sua chave pública correspondente e, são assinados digitalmente pela CA.

M.Silva *et al* (2003: 160) define a Autoridade Certificadora como "uma entidade que se encarrega de verificar os dados presentes num certificado digital e que o assina, confirmando a exactidão dos dados". Nesse caso, deverá ser pessoa, empresa ou outra entidade que transmita confiança aos utilizadores, para assim, emitirem par de chaves.

Segundo P.Silva *et al* (2003) o utilizador final para obter o certificado, terá que registar junto da CA. Uma vez registado, este recebe informação exclusiva que o autentica. É criado então o par de chaves (público/privado). Por fim, o utilizador faz o pedido formal do certificado digital, onde é associado ao par de chaves informações de identificação deste.

Para os mesmos autores (*idem*) existem várias situações em que os certificados podem ser revogados nomeadamente quando: estes possuem uma validade previamente definida depois da qual deixam de produzir efeitos; quando uma chave é comprometida, torna-se pois, necessário proceder-se à sua invalidação. Compete a CA, após a revogação, emitir listas de certificados inválidos e disponibilizar essas listas a toda a comunidade de utilizadores.

5.9 VLAN

Molinari (s.d) citado por Moraes (2002) afirma que "uma rede virtual é um grupo de estações e servidores que se comunica independentemente de sua localização física ou topologia, como se fosse um único domínio *broadcast*, ou uma rede lógica". Esta rede local constituída por um conjunto de máquinas lógicas, permite que utilizadores fisicamente distantes estejam conectados a mesma rede e se comunicam com maior segurança e rapidez, limitando o domínio de *broadcast* (quando uma estação transmite pacotes de dados a todas as outras estações de rede, sem qualquer restrição dos destinatários da mensagem, isto é, mesmo que o objectivo seja alcançar somente um *host*, manda mensagem para todos).

Moraes (2002) aponta alguns benefícios na utilização de VLAN nomeadamente:

- Controle do tráfego de *broadcast*: a redução do número de pacotes remetida a destinos desnecessários, resulta numa melhoria de capacidade de toda a rede. Além disso uma rede segmentada contém menor domínio de *broadcast*, devido ao menor número de dispositivos pertencentes a cada segmento.

- Segmentação lógica da rede: mesmo estando os utilizadores fisicamente separados, as VLANs possibilitam uma segmentação lógica da rede.

- Redução de custos e facilidade de gerir: a movimentação ou adição de máquinas ou utilizadores é feita de forma lógica sem exigir mudanças físicas, o que traduz numa alta flexibilidade, facilidade no processo e a redução de custos.

- VLANs funcionam utilizando a conexão lógica o que lhe proporciona uma independência da topologia física da rede.

- Maior segurança: VLANs limitam o tráfego a domínios específicos, os pacotes de comunicação da rede são entregues unicamente ao destino pretendido, dificultando o acesso a possíveis invasores e somente o tráfego desejado passa pela VLAN. Desta forma, o tráfego que circula numa VLAN não pode ser acedido por outra, assim como fica restrito o acesso a servidores pertencentes a VLANs diferentes.

5.10 VPN ou redes privadas virtuais

O *firewall* protege dados que entram e que saem da rede interna, contudo depois dos dados deixarem a área protegida pelo *firewall*, informações sensíveis como *password*, número de contas bancárias, etc., podem ficar susceptíveis de serem visíveis por acesso de terceiros. As VPN permitem a utilização da rede pública para a transmissão segura de informações.

Para Monteiro e Boavida (2000: 363) “uma rede virtual privada é uma rede constituída por um conjunto de redes privadas interligadas por circuitos/canais virtuais suportados noutras redes – normalmente públicas – como, por exemplo, a Internet”. Ou seja, uma rede privada construída sobre a infra-estrutura de uma rede pública, mas devido a utilização de tecnologias de tunelamento e outros procedimentos de segurança, fazem com que as mesmas sejam redes seguras. VPN garantem, assim, a utilização de redes de comunicação não segura

para trafegar informação de forma segura, pois toda a informação que circule pela internet e cujo destino seja uma rede privada, está criptografada.

De acordo com Monteiro e Boavida (2000), existem três tipos distintos de soluções para a implementação de VPN:

- baseadas em *firewalls*, partindo do princípio que o *firewall* é um dispositivo que já existe numa rede privada, há uma economia de recursos, uma melhor gestão (existe um ponto único de implementação de segurança) e verificação das condições de segurança. Apesar do *firewall* sofrer degradação no seu desempenho devido às funções (de codificação e descodificação) das VPN, esta é a solução mais utilizada.

- baseadas em *routers*, neste caso não há degradação no desempenho do *firewall*, porque as VPN estão baseadas nos *routers*, possibilitando também uma economia de recursos, (pois os *routers* são dispositivos de rede), mas não comprometendo o desempenho dos *routers*. Contudo a funcionalidade das VPN implementada acima do nível de rede, não pode ser suportada nos *routers*.

- baseadas em *software*/*hardware* dedicado, utilizado normalmente quando nem *firewall*, nem *routers* suportam as sessões VPN, ou seja, passa a existir mais um sistema para gerir e configurar e mais um ponto de implementação das funções de segurança.

Mamede (2006) defende que existem vários protocolos que estão associados às VPN, entre os quais destacam-se:

- PPTP, permite apenas uma ligação ponto-a-ponto por sessão e fornece um meio seguro de ligação de clientes individuais a servidores;

- L2TP, surge da combinação do PPTP e L2F (um dos primeiros protocolos utilizados por VPN, permite a ligação entre utilizadores remotos), foi concebido para a ligação ponto-a-ponto entre um cliente e servidor;

- GRE, utilizados entre routeadores.

- IPSEC (IP *Security*), é o protocolo essêncial para garantir a segurança de comunicação entre redes, criado pelo IETF (organização responsável pela criação dos protocolos padronizados para a internet). Segundo Mamede (*idem*) o protocolo IPSec possui a funcionalidade de cifrar e autenticar os dados do pacote IP. A implementação correcta deste protocolo garante confidencialidade, integridade, autenticidade e protecção contra o processamento duplicado de pacotes.

A utilização de VPN traz vários benefícios entre os quais pode-se citar o facto de já oferecer recursos de autenticação e criptografia, possibilita a transmissão segura de dados entre redes; redução de custos em comparação com a utilização de conexões dedicadas, etc.

A segurança física e a segurança lógica garante que os recursos físicos e os *softwares* estejam protegidos, contudo para que a segurança informática seja garantida importa fazer referência a segurança dos recursos humanos, pois muitos dos erros ocorridos têm origem nos recursos humanos de uma organização.

6 Segurança dos recursos humanos

Quando se fala em segurança informática há que levar em consideração um aspecto muito importante que são os recursos humanos, pois são estes que interagem directamente com os recursos tecnológicos, com os sistemas e gerem a informação dentro da organização. Muitos dos problemas de segurança acontecem internamente e, são na maioria das vezes causados (acidental ou intencionalmente) por colaboradores sem a formação mais adequada, falta de experiência, negligência, insatisfação na definição do plano de carreira e salário, entre outros. Para desenvolvimento deste ponto, alguns subpontos serão aqui objectos de análise como o recrutamento, a formação, a segregação de responsabilidades.

6.1 Recrutamento

A segurança dos recursos humanos, deverá começar desde a selecção dos candidatos com os melhores requisitos para preencher os postos de trabalho disponibilizados pela organização, particularmente para os que irão lidar com informações críticas, as exigências deverão ser

acrescidas relativamente a questões de segurança. Como afirmam Ferreira e Alves (1995) "candidaturas para admissão devem ser examinadas em pormenor sempre que os postos de trabalho envolvam o acesso a recursos das TI que manipulem informação sensível". Aliás, Mamede (2006: 53) sublinha que "uma organização não pode correr o risco de admitir pessoal que possua um registo de criminalidade informática ou de atitudes pouco concordantes com a ética, em outras organizações".

P.Silva *et al* (2003) afirmam que aquando da contratação de um novo colaborador, este deverá receber todas as informações que lhe permita estar a par do conjunto das normas, regras e princípios existentes na organização, sobre as suas permissões e o que lhe é proibido fazer. Isso é realizado através de um acordo entre o colaborador e a organização que compromete o cumprimento de ambas as partes. Esta atitude permite impedir que posteriormente possam surgir afirmações de alegado desconhecimento dos princípios estipulados pela organização.

A segurança dos recursos humanos apresenta os seguintes objectivos, de acordo com Mamede (2006: 30):

> (…) reduzir os riscos de erro humano, roubo, fraude ou utilização indevida de qualquer parte do sistema; assegurar que os utilizadores estão sensíveis às ameaças à segurança da informação e que estão devidamente equipados para suportar a política de segurança da organização no decurso normal das suas actividades; minimizar os danos de incidentes de segurança e mau funcionamento e aprender com esses mesmos incidentes.

6.2 Formação/sensibilização

Para a concretização dos objectivos acima mencionados, é fundamental a questão de informação e formação/sensibilização de todos os colaboradores, principalmente dos que lidam com informações críticas, estes precisam ter um nível mais elevado de sensibilização para as questões de segurança. Como afirma Mamede (2006: 54) " (…) a formação em segurança deve ser disponibilizada a todos os colaboradores que concebam, implementem ou efectuem a manutenção de sistemas de rede, bem como a todos os colaboradores da organização, sensibilizando-os para os variados problemas".

O objectivo da formação segundo Ferreira e Alves (1995: 79) é “garantir que os utilizadores têm consciência das ameaças e preocupações respeitantes à segurança da informação e estão sensibilizados para apoiar a política de segurança da organização (…) ”. Silva (2005) reforça dizendo que de nada adianta disponibilizar tecnologias se “os usuários dos sistemas da organização não estiverem conscientes da importância da segurança da informação e do correcto uso destes sistemas”.

Por seu lado, P.Silva *et al* (2003) referem à necessidade de acções de sensibilização sobre questões concretas dos problemas relacionados com a segurança do dia-a-dia da organização. Uma das questões importantes a levar em conta é a de engenharia social.

A engenharia social segundo Mamede (2006: 116) “consiste na aplicação de truques, psicológicos ou físicos, sobre utilizadores legítimos de sistemas computacionais, de forma a obter-se conhecimento e informação que permita acesso a esse sistema”. Como se pode notar, a engenharia social constitui uma estratégia de recolha de informações sem exigir perícia técnica. Esta forma de ataque pode concretizar-se de diversas formas: muitas vezes, atitudes de entreajuda humana no ambiente laboral podem comprometer informações sensíveis, alguém pode passar-se por terceiro podendo obter informação relevante de colaboradores com falta de formação/sensibilização, o fornecimento de informações sensíveis como por exemplo uma *password*, pode reverter, muitas vezes, em prejuízos avultados para a organização.

Para além da engenharia social, outros problemas podem estar associados a segurança dos recursos humanos, tais como *Caller ID spoofing* e Mergulho no contentor (*Dumpster Diving*). *Caller ID spoofing* tem por objectivo fazer uma chamada telefónica com um número de telefone falso, através de servidores na internet que permitem falsificar ID de telefone, fazendo com que apareça o número que nós quisermos no visor do destinatário.

Para evitar a engenharia social e *caller ID spoofing*, uma organização deve investir na formação dos seus colaboradores sobre questões de segurança e na sensibilização dos mesmos para não partilharem informações sensíveis com terceiros ou através de chamadas telefónicas simpáticas.

Segundo P.Silva *et al* (2003) o mergulho no contentor consiste na procura de informações sensíveis vasculhando o lixo da organização. Parte desse lixo que pode ser código de algum cartão, listagens de números de telefones, impressões de configurações de equipamentos, entre muitos outros, que podem servir de base para um posterior ataque. Como mecanismo de defesa a este tipo de ataque aconselha-se a utilização de destruidor de papel ou alternativamente fornecer a cada colaborador um sexto para a colocação de materiais sensíveis. E estes seriam posteriormente destruídos de forma adequada.

É igualmente importante a definição de um plano de carreira e salário capaz de motivar o colaborador naquilo que ele faz. Convém ressaltar que para além da remuneração directa (salário), há a remuneração indirecta (planos de benefícios: recompensa ou beneficio social como subsidio de férias, abono de família, etc.).

6.3 Segregação de responsabilidades

P.Silva *et al* (2003) defendem que se deve evitar atribuir funções vitais a uma única pessoa, estas devem ser atribuídas a pelo menos duas pessoas. A possibilidade de falhas ou erros nas organizações podem muitas vezes estar relacionada com a concentração de actividades ou funções críticas a única pessoa. No caso de ausência destas pessoas ou de ocorrência de algum erro por parte destes, a organização pode comprometer o seu funcionamento.

Se até aqui procurou-se perceber o conceito de segurança informática, bem como outros conceitos afins, a segurança física, lógica e de recursos humanos, de seguida vai-se incidir sobre o planeamento da segurança, ou seja, a política e os planos de segurança.

7 Planeamento de segurança

7.1 Políticas de segurança

Ferreira e Araújo (2006) citados por Pinheiro (2007) afirmam que “a política de segurança define o conjunto de normas, métodos e procedimentos utilizados para a manutenção da segurança da informação devendo ser formalizada e divulgada a todos os usuários que fazem

uso dos activos de informação". De acordo com esta definição, todas as normas e regras referentes à segurança informática devem ser abordadas por políticas explícitas, ou seja, deverá existir um documento formal que especifique um conjunto de regras e normas que definem o processo da segurança informática. É importante, também a definição das sanções em caso de violação das normas e regras da política definida e como serão aplicadas.

Segundo Hartley e Locke (2001) citados por Mamede (2006), para se desenvolver uma política de segurança deve-se levar em conta as seguintes actividades:

- avaliação e entendimento das necessidades de segurança: há a necessidade de fazer a recolha de informações e fazer uma análise e gestão de risco, definir as prioridades de segurança, tendo em conta o factor custo/beneficio;
- revisão das políticas em vigor, caso existam: o documento de política de segurança deve ser periodicamente examinado por especialistas, para se fazer as possíveis actualizações à medida que vão acontecendo as mudanças organizacionais tanto internas como externas;
- definição dos requisitos de protecção: definir que recursos se deve proteger e como;
- formalização da política de segurança: elaboração do documento formal que define a política de segurança da organização.

A definição da política de segurança, é sempre específica para cada organização, contudo Medeiros (2001) defende que existem pontos comuns para todas as organizações nomeadamente: fazer uso da informação como um bem da empresa; definir claramente as responsabilidades de segurança na organização; definir as medidas disciplinares, caso a política não seja cumprida; não pôr em causa a privacidade do utilizador; definir o controlo de acesso; especificar as condutas em situações de contingência.

Carneiro (2002) defende que a política deve ser definida de forma clara, precisa e concisa de modo que todos os seus destinatários possam entender, esta política deve ser divulgada, através de um programa de sensibilização, de modo que seja de conhecimento geral. Para além disso, a política de segurança deve ser definida tendo em conta os objectivos da

empresa e deve ser possível de ser posta em prática, tudo isso no sentido de possibilitar um grau de envolvimento e comprometimento maior por parte dos colaboradores.

7.2 Planos de segurança

Mesmo com os melhores mecanismos de segurança implementados, a organização pode estar sujeita a ameaças ou riscos que podem ter fontes diversificados, daí advém a necessidade de planos que especificam os procedimentos que garantem o funcionamento das actividade críticas e a continuidade de serviço face a ocorrências anormais, bem como as prioridades em caso de qualquer acidente ou desastre. Definir planos de segurança corresponde a disponibilizar a organização de meios para dar resposta em caso de incidentes de segurança, minimizando os custos de restauração.

Neste sentido Ferreira e Alves (1995: 47) defendem que o objectivo da formulação do plano de segurança é "garantir que as actividades críticas da Organização sejam restabelecidas e mantidas o mais rapidamente possível a seguir a qualquer desastre ou falha importantes que afectem recursos ou serviços essenciais".

O plano de segurança pode ser composto pelo:

- plano de contingência;
    - plano de reposição;
    - plano de recuperação.

7.2.1 Plano de contingência

O plano de contingência permite garantir a continuidade das actividades críticas do funcionamento da organização, ou seja, assegurar que entre ocorrências anormais (destruição por fogo, inundação, interrupções acidentais, etc.) e a retoma do pleno funcionamento das actividades, a organização continue a desempenhar as suas actividades críticas.

A elaboração deste plano deve ser antecedida com uma análise de risco que permite por um lado, pôr em evidência o que é essencial para a manutenção da continuidade das actividades organizacionais e, por outro, fazer uma análise custo/beneficio.

Objectivos do plano de contingência segundo Ferreira e Alves (1995) são:

- assegurar o funcionamento das actividades críticas da organização no período entre a ocorrência do incidente e a reposição total da situação inicial;
- minimizar os danos e prejuízos financeiros;
- estabelecer acções que permitam a reposição total dos recursos das TI bem como o normal funcionamento de todas as suas actividades.

Diante da grande variedade de ameaças que uma organização está sujeita, é impossível evitar todas as formas de ataque contudo, o documento de contingência é uma medida preventiva que permite limitar as consequências dos danos que podem surgir. Não existe assim, um único plano de contingência, mas vários planos intermédios para dar resposta a diferentes situações de sinistro. Assim sendo, os planos de recuperação e de reposição constituem os sub-planos do plano de contingência.

Em situações extremas pode-se recorrer a instalações alternativas que de acordo com Simões (2004) podem ser: *cold centers* (sala de computadores com infra-estruturas básicas), *worms centers* (sala com sistemas informáticos e outros equipamentos para situações de emergência), *hot centers* (centro de processamento alternativo já operacional).

O plano de reposição é um documento que descreve as normas para repor o normal funcionamento da organização em situações de alguma avaria ou interrupção. Para Ferreira e Alves (1995) o plano de reposição pode aplicar-se em caso de ocorrências de incidentes dos seguintes tipos:

- avarias no equipamento;
- avarias de climatização ou de energia eléctrica;
- avarias ou erros de telecomunicações;

- erros de programação ou de exploração;
- destruição de ficheiros;
- ausência de pessoal.

Perante tais situações um conjunto de medidas deve estar já materializado tais como ter *stock* de equipamentos, ter sistema UPS pelo menos nos equipamentos críticos, ter sistema antivírus centralizado e actualizado, etc.

O pano de recuperação, segundo P.Silva *et al* (2003: 154) "é um documento composto pelas descrições das respostas a uma interrupção nas actividades, processos e funções importantes do negócio, que se prolongue para além das respectivas tolerâncias à indisponibilidade".

O objectivo principal deste plano é criar cópia de segurança de toda a informação relevante. Para tal deve-se seguir um conjunto de procedimentos e Ferreira e Alves (1995) citam os seguintes que devem ser estabelecidos pelo responsável pelo sistema informático:

- periodicidade das cópias de segurança: a periodicidade das cópias pode ser diária, semanal, mensal, anual, ou de periodicidade variável;
- número de exemplares das cópias de segurança;
- localização de arquivos de suporte magnético: a localização do armazenamento das cópias de segurança, deve ser feita tendo em conta não só a segurança, mas também a disponibilidade, sempre que haja condições essas cópias devem ser guardadas em lugar distinto dos dados originais;
- procedimentos de reposição.

Todo o procedimento para a recuperação e salvaguarda da informação deve constar num documento que descreve todos os detalhes da realização das cópias de segurança, como por exemplo: que ficheiros ou informação deve ser copiado, como deve ser; o momento em que deve ser efectuado a cópia; quem deve efectuar as cópias; cifrar as cópias de segurança sempre que houver condições para tal, entre outros.

A redundância surge como forma de evitar a indisponibilidade da informação e deverá ser efectivada, levando em conta o valor da informação que se quer proteger. P.Silva *et al* (2003: 101) afirmam que "na sua expressão mais complexa, estes mecanismos de protecção podem assumir a duplicação total da infra-estrutura informática existente, numa localização remota, com transferência automatizada de dados entre locais". Contudo, este tipo de implementação exige elevados custos e manutenção e que por isso está voltada para estruturas críticas.

Para colmatar tal situação, a solução mais comum é a criação de *clusters* de máquinas e pela implementação de RAID. *Cluster* segundo Mamede (2006: 372) "é um grupo de computadores independentes que se combinam para trabalhar como um sistema único redundante", ou seja, são vários servidores que trabalham como se fossem um só e quando houver indisponibilidade de um, o outro entra em funcionamento de imediato. RAID significa que a informação encontra-se partilhada por vários discos, se um desses deixar de funcionar, os dados poderão ser acedidos num outro disco.

Carneiro (2002) aponta alguns benefícios de um plano de segurança tais como: aumento da produtividade; aumento da motivação do pessoal; comprometimento com a missão da organização; melhoria das relações de trabalho; contribuição para a formação de equipas técnicas competentes.

8 Considerações finais

Considerando a segurança informática um conjunto de medidas que são tomadas para garantir que os recursos das TI sejam protegidos contra diferentes tipos de ataques, ela não pode ser encarada simplesmente como um produto ou uma tecnologia que se adquire e aplica, mas sim como um processo capaz de acompanhar a permanente evolução do mundo tecnológico e tem como objectivos principais garantir os princípios de autenticidade, disponibilidade, integridade e disponibilidade.

Pode-se referir a segurança informática em três níveis importantes: segurança lógica, segurança física e segurança de recursos humanos. Enquanto que, a segurança lógica refere-se ao conjunto de medidas que devem ser levadas a cabo para proteger os *softwares*, os dados/informações, a segurança física destina-se a proteger os recursos físicos. Se a

segurança física for quebrada/corrompida, isso implica que todo o investimento em segurança lógica cairá por terra. Paralelamente aos recursos físicos e lógicos, estão os recursos humanos, factor de extrema importância na garantia da segurança informática, pois são eles que interagem directamente com os recursos das TI, e que por isso têm que estar sensibilizados e ter formação adequada para lidar com questões de segurança. A verdade é que não se pode dizer que nenhum dos níveis de segurança é mais importante de que outro, pois todos têm a sua importância e devem funcionar de forma integrada.

As normas e regras que especificam como a segurança deve ser garantida nos três aspectos supracitados, bem como as sanções no caso do incumprimento de tais normas e regras devem constar num documento formal – política de segurança. Este documento deve ser de conhecimento geral e estar escrita de forma clara e concisa.

Perante situações de acidentes, desastres naturais ou falhas técnicas e como forma de minimizar os impactos dos danos que podem afectar uma organização, é importante uma atitude pró-activa, ou seja, definir um plano de segurança: contingência (reposição, recuperação), dispor da existência de mecanismos que assegurem a sobrevivência das organizações face a tais situações.

Capítulo 2: Auditoria Informática

1 Enquadramento

Como viu-se no capítulo anterior a segurança informática deve ser vista como um processo devido sobretudo as mudanças que constantemente ocorrem no mundo das tecnologias e que influenciam o comportamento das organizações. Essa rápida evolução das tecnologias e a dependência cada vez maior das mesmas por parte das organizações leva a uma necessidade cada vez maior de controlo, ou seja, uma revisão periódica a um sistema informático, que se materializa através de uma auditoria informática.

Esta que constitui, com efeito, objecto de discussão, neste capítulo. Para isso começa-se por definir a auditoria informática, passando pelas suas estratégias, objectivos e, apresentando ainda alguns testes a ter em conta numa auditoria e por fim refere-se a alguns padrões internacionais para realização de auditorias.

2 Conceito da auditoria informática

Para Il Tec (1993), a auditoria informática define por uma “análise exaustiva de funcionamento de um centro de processamento de dados e do seu ambiente”. Por seu lado, Carneiro (2004: 21) afirma que “ (…) a auditoria informática é um conjunto de procedimentos e de técnicas para avaliar e controlar total ou parcialmente um sistema

informático". Partindo destas duas definições, pode-se concluir que a auditoria permite analisar, validar e avaliar o grau de protecção do sistema informático em todos os seus aspectos, verificar a conformidade com os objectivos e políticas da organização, ou seja, verificar se as regras, normas e procedimentos estabelecidos na política de segurança, estão sendo aplicadas no dia-a-dia da organização. Sendo assim, a auditoria permite a uma organização clarificar o que está na base das vulnerabilidades e ajuda na tomada de acções que permitem colmatar as mesmas. Ou aliás, conforme afirma Mamede (2006: 416) "a auditoria faz parte integrante do processo de segurança na organização, na medida em que permite avaliar a implementação da política de segurança e identificar lacunas e omissões na mesma, permitindo a introdução de alterações e ajustes na mesma (…)".

A auditoria informática segundo Carneiro (2004: 17) apresenta os seguintes objectivos:

- inventariar e avaliar os meios físicos e as tecnologias adequadas à recolha e processamento dos dados necessários à obtenção das informações necessárias;
- examinar a existência de controlos apropriados e avaliar a sua eficácia;
- concluir sobre a qualidade e a utilidade da informação obtida;
- garantir a montagem e adequação de procedimentos e sistemas de controlo que assegurem a segurança do SI na sua relação directa com os materiais informáticos (*hardware* e *software*).

Contudo, a concretização destes objectivos exige não só a definição de metodologias e técnicas específicas, mas é preciso também que o auditor disponha tanto de conhecimentos técnicos como de algumas aptidões como destaca este mesmo autor (*idem*) a honestidade, objectividade, aptidão crítica, capacidade de análise e síntese, flexibilidade, comunicação com clareza, tendência a actualização dos conhecimentos, possibilidade de compreender rapidamente, capacidade de iniciativa e criatividade. A recolha de informação pode ser feita recorrendo a várias estratégias, conforme descreve o ponto seguinte.

3 Estratégias da auditoria

A implementação de uma auditoria exige que seja antecedida pela criação de um ambiente propício para tal. De igual modo, a recolha de informações, que pode vir de diversas formas e fontes, deve levar em conta uma escolha adequada de estratégias. Neste sentido, Carneiro (2004) destaca as seguintes estratégias para a realização de uma auditoria: questionários, entrevista e *checklist*.

3.1 Questionário

Os questionários são técnicas de recolha de informação e consistem numa série ordenada de perguntas, podendo ser respondidas sem a presença do auditor. Segundo o pensamento de Gil (1999: 70) o questionário "corresponde à elaboração de um conjunto de perguntas com o objectivo de verificação de determinado ponto de controlo do ambiente computacional".

De acordo com Carneiro (2004: 72) os questionários devem ser "cuidadosamente elaborados quer em conteúdo quer no que se refere à forma, é muito aconselhável que estes questionários sejam muito específicos para cada situação". Tudo isso, para que seja de fácil entendimento por parte do auditado, podendo assim obter as respostas que se pretende.

Gil (1999) afirma ainda que o facto dos questionários poderem ser aplicados a distância, podem estar sujeitos a interpretações subjectivas, contudo este tipo de estratégia possibilita um diagnóstico para depois obter maiores níveis de detalhes, quando a sua aplicação se faz juntamente com outras técnicas como a entrevista.

3.2 Entrevista

A entrevista constitui um outro instrumento de recolha de informação e baseia em questões, previamente preparadas, em que o entrevistado na presença do entrevistador responde, podendo ser entrevistas abertas ou fechadas. Conforme afirma Carneiro (2004) as entrevistas assumem de duas formas: uma em que o entrevistador utiliza um método pré-estabelecido, as questões estão estruturadas e com finalidades bem definidas e, outra em que o entrevistado fornece todas as informações mediante um tema proposto pelo entrevistador, é a entrevista semi-dirigida, em que o entrevistado tem liberdade para expor as suas ideias.

Segundo Ferreira *et al* (2001) as modalidades de entrevistas podem ser: contacto pelo correio, contacto telefónico e contacto directo. A remessa de carta via correio normalmente não é propriamente considerada uma entrevista, mas faz-se necessário quando o universo é muito grande e disperso geograficamente, reduzindo custos mas o número de respostas é muito baixo dificultando a análise dos resultados obtidos.

O contacto telefónico é utilizado quando se pretende abranger um grande número de pessoas num curto espaço de tempo, deve variar entre 30 a 15 minutos, sendo o ideal de apenas 15 minutos.

Nas entrevistas de contacto directo se pode beneficiar de aspectos importantes para estabelecimento do ambiente propício para trocas de informação, aspectos esses que não estão presentes nos dois tipos de entrevista acima citados, como a observação do entrevistador das reacções não verbais do entrevistado e o calor humano.

Neste último caso, o entrevistador deverá ter habilidade de criar um clima de confiança e cooperação mutua através de um contacto amistoso com o auditado. As entrevistas devem ser previamente preparadas e o auditor não deve influenciar o sentido das respostas, pois esta constitui a forma de complementar a informação fornecida na aplicação dos questionários e, por isso, um dos momentos em que o auditor obtém informação relevante para o seu processo de análise.

3.3 Checklist

De acordo com Carneiro (2004) as *Checklist* são conversas informais ou conjunto de perguntas de formulação flexível que conduzem o auditor a respostas coerentes que permitem uma correcta descrição dos pontos fracos e fortes. Igualmente como as entrevistas, as *checklists* complementam as informações fornecidas pelos questionários. O mesmo autor (*idem*: 73) afirma que “regra geral, as *checklist* devem ser respondidas oralmente, pois podem fornecer conteúdos mais individualizados e mais ricos do que as outras formas”.

Apesar da decisão para realizar uma auditoria, depender das circunstâncias específicas de cada organização, P.Silva *et al* (2003) afirma que se deve escolher a altura adequada para a realização de uma auditoria de segurança e aponta algumas possibilidades nomeadamente: aquando da nomeação do responsável pela segurança; após a implementação de medidas de segurança; com regularidade temporal e ainda em outras situações de testes pontuais. A auditoria pode ser interna ou externa como a seguir se descreve.

4 Auditoria interna e auditoria externa

O processo de realização de uma auditoria é tanto complexo, quanto maiores forem os ambientes organizacionais, com muitos postos de trabalho, com redes muito complexas, etc. Para Carneiro (2004) uma auditoria pode ser realizada por recursos internos, são os funcionários da organização a ser auditada (auditoria interna) como por consultores externos, que são as entidades que não pertencem à organização auditada e normalmente com dedicação exclusiva em firmas de auditoria (auditoria externa). O mesmo autor (*idem*: 8) afirma que a auditoria interna tem por função auxiliar a equipa de gestão no seu desempenho, enquanto que, a auditoria externa é realizada normalmente quando se pretende "uma maior objectividade relativamente à auditoria interna, devido a um maior distanciamento entre auditores e auditados".

Comparativamente com a auditoria externa, a auditoria interna segundo Ferreira *et al* (2001) apresenta algumas vantagens as quais podemos sublinhar algumas: não são tão perceptíveis aos funcionários quanto as auditorias externas; são mais económicas, pois neste caso, os auditores já conhecem o sistema a ser analisado; actuam muito rapidamente nos casos de emergência; são fortes fontes de consulta actualizada; constituem ponto de apoio e base para as auditorias externas; entre outros.

Apesar de todas as vantagens da auditoria interna mencionadas, Mamede (2006) afirma que as melhores auditorias são realizadas por auditores externos sem quaisquer ligações ao ambiente da organização, por estarem menos sujeito a influência de subjectividade na produção dos resultados do processo.

Quer no caso da auditoria interna, como no da auditoria externa, segundo este mesmo autor (*idem*), é importante que a equipa dos auditores seja imparcial, ou seja, não deverão existir problemas de relacionamento pessoal entre os auditores e os auditados para não interferir nos resultados do processo e possam traduzir a realidade da organização.

O recurso a auditoria interna e a auditoria externa em simultâneo denomina-se, segundo Ferreira *et al* (2001), de auditoria articulada, esta que constitui numa mais rica forma de recolher informações sobre o sistema informático de uma organização.

Conforme afirma Carneiro (2004: 114) “a auditoria da segurança do sistema pode referir-se à segurança global de toda a instalação ou à segurança de uma área particular e denomina-se então segurança específica”. Isto quer dizer que, de acordo com as necessidades de cada organização se pode fazer uma análise específica a cada área, ou então, pode ser feita uma análise completa e exaustiva de todo o sistema informático. Este último, como afirma P.Silva *et al* (2003), por ser mais abrangente, demora mais tempo e é também mais dispendioso, podendo os resultados deste tipo de auditoria ser bastante volumosos, mas é importante que sejam resultados úteis. Tendo em conta as diferentes possibilidades de testes e auditoria, entende-se aqui fazer referência a três áreas principais, que de certa forma acabam por abranger os recursos (lógicos, físicos e humanos) que devem ser examinados/analisados no decorrer de uma auditoria informática.

5 Principais áreas da auditoria informática

5.1 Auditoria em segurança física

A segurança física, uma das áreas a ser analisada numa auditoria informática, possibilita aos auditores verificar a conformidade dos procedimentos, medidas e princípios utilizados com os especificados pela política de segurança referente aos recursos físicos. Carneiro (2009: 183) afirma que “esta auditoria avalia as proteções físicas de dados, programas, instalações, equipamentos, redes e suportes, e considera também a integridade física dos utilizadores, por exemplo, condições de trabalho, medidas de evacuação, alarmes e saídas alternativas”.

Aquando da realização de uma auditoria na segurança física, de acordo com Mamede (2006) deve ser levado em consideração um conjunto de tarefas, as quais se destacam:

- verificação dos sistemas de energia: deverão verificar se existem sistemas de alimentação e protecção adequados; se os equipamentos críticos dispõem de sistemas de alimentação ininterrupta de energia eléctrica que suportam o seu funcionamento por um determinado período de tempo; se os não críticos estão ligados a estabilizadores de corrente eléctrica;

- verificação das condições ambientais: devem ser verificadas as condições ambientais nas salas onde residem os equipamentos informáticos, ou seja, se existem

mecanismos que permitem controlar quer o calor, quer a humidade e se existem sistemas de alerta em caso de alteração das condições ideais;

- verificação dos controlos de acesso físico: deverão ser auditados aspectos tais como verificar se as salas dos equipamentos informáticos e particularmente os dispositivos críticos dispõem de controlos de acessos adequados, permitindo o acesso às mesmas apenas pessoas autorizadas;

- verificação da existência de equipamentos e de planos de emergência: desses equipamentos deverão constar os extintores, alarmes de fogo e intrusão e, ainda deverão verificar se tais equipamentos são regularmente testados;

- nível de monitorização física das localizações: os auditores deverão verificar a presença de guardas, sistemas de vídeo-vigilância, sensores de portas, sistemas de registos que permitam controlar as entradas e saídas;

- cablagem e montagem de elementos físicos: verificar em todas as áreas onde existem equipamentos se os cabos estão montados de forma organizada e com a devida identificação e certificar-se de que os mesmos encontram-se em locais de acesso controlado, para evitar a indisponibilidade dos serviços.

5.2 Auditoria em segurança lógica

Grande parte dos ataques é realizada a nível das aplicações e dos dados, daí a necessidade de serem verificados periodicamente os aspectos referentes a manutenção da segurança lógica, ou seja, validar e avaliar se os vários aspectos referentes a segurança lógica existem e se estão em conformidade com os procedimentos definidos pela política de segurança da organização. Quando se pretende efectuar uma auditoria de segurança lógica devem ser considerados vários aspectos, os quais passamos aqui a fazer referência.

O controlo de acesso é um dos aspectos importantes a ter em conta nesta auditoria e segundo Fegundes (2004) é o ponto mais suscetível a falhas. Para Dantas (2010) o objectivo do controlo de acesso é “(…) proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por usuários ou outros programas”. Nesse sentido, a auditoria de controlo de acesso lógico permite identificar e reduzir falhas de acesso aos recursos. Este

mesmo autor acrescenta alguns procedimentos a ter em conta neste tipo de auditoria, tais como "(…) utilizar software de controle de acesso; desabilitar as senhas de ex-funcionários; não armazenar senhas em log; desabilitar contas inativas (…)". Pode-se afirmar, neste caso, que o auditor tem a tarefa de analisar como é feita a gestão das contas dos utilizadores, desde o momento da sua criação, respeitando os requisitos de segurança definidos até a sua desactivação, verificando se apenas utilizadores autorizados possuem acesso ao sistema.

Apesar de hoje estar a ser utilizados outros métodos de autenticação e controlo de acesso, tais como o método de biometria, o método mais utilizado, segundo Carneiro (2009), é o de *password*, neste particular, deverão ser verificadas se as políticas para a sua definição e utilização estão sendo aplicadas de acordo com as normas e padrões definidos pela organização. Torna-se assim necessário considerar que não é suficiente apenas a utilização de sistemas de *password*, mas é igualmente importante que numa rede de computadores, as políticas existentes evitem que as *password* sejam fáceis de adivinhar pois, como Mamede (2006: 439) argumenta, "uma palavra-passe fraca é o suficiente para ultrapassar com sucesso por todas as configurações seguras de servidores, actualizações de sistemas e regras de *firewall* muito apertadas".

Para detectar tentativas de acesso não autorizado a um sistema P.Silva *et al* (2003) afirmam que devem ser realizados testes de intrusão, podendo ser realizados tanto do interior da rede da organização, como a partir da organização. O auditor pode, num cenário mais realista, assumir o papel de hipotético atacante, nesse caso ele não tem qualquer conhecimento do sistema a testar ou, pode obter o conhecimento completo das características do sistema a analisar e consequentemente irá detectar maior número de vulnerabilidades.

Mamede (2006) afirma que devem tentar localizar todas as vulnerabilidades existentes através dos acessos a serviços internos e ressalta que os pontos mais vulneráveis de acessos a serviços internos são as ligações internet, *modems* activos, pontos de acesso sem fio e pontos de acesso através de rede virtual privada, desta forma a auditoria deve ser alargada a todos estes pontos, para evitar que elementos não confiáveis possuem acessos a recursos internos.

Para que tal acontece o mesmo autor (*idem*) destaca um conjunto de tarefas a serem realizadas pelos auditores, nomeadamente: localizar os dispositivos que estão visíveis e

sujeitos a tentativas de intrusão e suas vulnerabilidades directas, estes podem ser: *routers*, *switches*, servidores, entre outros; verificar a existência de várias camadas de segurança, se *firewall* e outros dispositivos de segurança encontram-se devidamente configurados e actualizados, verificando a sua conformidade com as políticas definidas pela organização; pesquisar pontos de entrada que não sejam conhecidos, por exemplo, localizar a existência de *modems* não autorizados na rede da organização.

O auditor deve ainda fazer uma auditoria às aplicações de uma organização, ou seja, verificar se as aplicações dispõem dos requisitos e se são implementados de acordo com as políticas de segurança vigentes. Assim sendo, alguns aspectos deverão ser analisados especificamente a política de actualização e a política de controlo de acesso. Tendo em conta que as aplicações disponibilizem acessos a dados, estas devem ser o mais seguro possível, evitando que informações críticas possam ser acedidas por entidades não autorizadas. Para evitar tal risco, Carneiro (2004) refere a importância de um controlo específico que permite que apenas utilizadores autorizados tenham acesso a funções concretas dentro das aplicações.

O *software* antivírus é outro aspecto importante a considerar numa auditoria de segurança lógica, nesse caso, segundo Mamede (2006) o auditor deve verificar a sua correcta utilização, ou seja, verificar se o antivírus está a executar-se normalmente; se o *software* antivírus é actualizado regular e automaticamente; se todos os serviços desnecessários estão desactivados; se foram aplicadas todas as actualizações ao sistema operativo.

Carneiro (2009: 187), argumenta que a continuidade das operações constitui um aspecto importante que se deve considerar numa auditoria de segurança, ou seja, para além de existir o documento sobre o plano de contingência, o auditor deverá certificar de que este plano funciona com as garantias necessárias e com idoneidade técnica “se é completo e actualizado, se cobre os diferentes processos, áreas e plataformas (…)”. Um outro ponto fundamental a ser validado numa auditoria de segurança, segundo o mesmo autor (*idem*), é a existência de cópias actualizadas dos recursos vitais, tais cópias devem situar-se em locais seguros e protegidas de acessos indevidos e devem possibilitar a reposição de sistemas.

Os computadores pessoais também considerados recursos tecnológicos da empresa devem ser analisados no decurso de uma auditoria informática. De acordo com Mamede (2006: 426)

"o objectivo de uma auditoria aos computadores pessoais é garantir que os controlos de segurança adequados estão instalados e que as políticas definidas para os utilizadores estão em prática". Este mesmo autor considera os computadores pessoais como extensões de servidores e de rede da empresa e, por isso, se estes apresentam vulnerabilidades, também os servidores e rede da organização podem estar vulneráveis.

O mesmo autor aponta alguns aspectos que deverão ser verificados neste tipo de auditoria tais como: se a ferramenta antivírus está instalada e actualizada; se existe um *modem* ou qualquer outra forma de acesso externo ligado ao sistema; se a utilização de *password* no computador pessoal está de acordo com a política de *password* da organização; se o disco rígido do computador contém informação sensível que deva estar armazenada num servidor seguro; se no computador estão instaladas ferramentas ou aplicações não autorizadas; se existem condições de transportar o mesmo para fora das instalações em segurança.

5.3 Auditoria em segurança dos recursos humanos

Segundo a norma ISO/IEC 17799 o objectivo da segurança de recursos humanos é reduzir riscos de erros humanos, roubos, fraudes ou uso indevido das facilidades. Importa, nesse sentido, referir que a auditoria de recursos humanos numa organização vem no sentido de garantir estes objectivos, cabendo ao auditor fazer um levantamento exaustivo dos requisitos da segurança de recursos humanos e verificar se estes estão sendo aplicados.

Um dos aspectos a verificar na auditoria em segurança dos recursos humanos é a possibilidade de ocorrência de ataques tais como a engenharia social. De acordo com P.Silva *et al* (2003: 129) "este teste tem como objectivo detectar o grau de vulnerabilidade da organização a 'ataques sociais'". São testes realizados com simples tentativas de recolha de informação pessoalmente, ou por telefone fazendo passar por terceiros, para ver até que ponto os utilizadores dos recursos das TI estão sensibilizados para aspectos de segurança.

Faz sentido, neste particular, considerar situações como a deficiente qualificação, omissões e descuidos dos recursos humanos, apontadas por Carneiro (2009), como aspectos a serem analisados numa auditoria. Assim, torna-se necessário ao auditor verificar se estão estipulados nas políticas de segurança da organização programas de sensibilização e

formação e se os mesmos estão sendo realizados, estimulando atitudes técnicas e de responsabilidade individual.

Mamede (2006) refere à necessidade da auditoria aos administradores dos sistemas, pois muitas vezes, por existir muita concentração de funções, esta sobrecarga pode levar ao incumprimento de algumas funções referentes a práticas de segurança da organização. Convém neste caso, segundo este autor (*idem*: 429) verificar pontos como por exemplo "criação de novas contas de acesso, alteração de privilégios de acesso e de palavras-passe, verificar as políticas de gestão de palavras-passe fracas e por todas as que não estão em conformidade com o estabelecido na política de segurança (…)"

Um outro ponto também importante a ser considerado nesta auditoria, para Carneiro (2009) é a existência de segregação de funções para impedir que perante a prática de uma fraude por parte de um colaborador, não lhe seja possível ocultá-la. Este autor (*idem*: 59) afirma que "a ausência ou inadequação da segregação de funções aumenta o risco da ocorrência de transacções erróneas, de alterações impróprias e de danos em recursos computacionais".

6 Alguns padrões internacionais de auditoria informática

6.1 CobiT

ISACA define CobiT como um conjunto de ferramentas de apoio que permite aos gestores definir uma política, com base nas boas práticas, para controlo de TI, por outras palavras, ajuda a controlar e compreender benefícios e reduzir os riscos associados a utilização das TI. É aceite internacionalmente como guia de boas práticas, ou seja, um modelo de referência para melhorar o controlo da utilização das TI numa organização e ajuda na atenuação dos riscos correspondentes. Pedro (2005) compartilha da mesma ideia e afirma que "o Cobit é um modelo orientado para a gestão das tecnologias de informação".

Partindo desses dois conceitos, podemos pois afirmar que o CobiT oferece um conjunto de processos baseado nas melhores práticas que se destina a apoiar tanto os gestores TI, assim como para os auditores de um Sistema de Informação.

Fegundes (2004) afirma que o "CobiT está orientado para auxiliar três audiências distintas:

- Gerentes que necessitam avaliar o risco e controlar os investimentos de TI em uma organização;
- Usuários que precisam ter garantias de que os serviços de TI que dependem os seus produtos e serviços para os clientes internos e externos estão sendo bem gerenciados;
- Auditores que podem se apoiar nas recomendações do CobiT para avaliar o nível da gestão de TI e aconselhar o controle interno da organização.

Apesar destas três audiências encontrarem-se interligadas, é sobre este último que, em particular interessa aqui referir, ou seja, o que se pretende é referir ao CobiT como um padrão das melhores práticas para a realização de auditorias, constituindo assim numa ferramenta importante para auxiliar uma organização na gestão controlada das suas TI.

A visão deste modelo, segundo Pedro (2005), " (…) sustenta que a sobrevivência das organizações depende da gestão efectiva da informação e da tecnologia". Gestão essa, que conforme afirma o mesmo autor está associada a quatro problemas: o aumento da dependência das organizações relativamente às TIC; o aumento das vulnerabilidades e ameaças, a que as organizações que lidam com as TIC estão sujeitas; escala de custos com o SI (Sistemas de Informação), ou seja, os investimentos cada vez maiores que as organizações de diferentes sectores fazem nas TIC; o grande potencial associado à utilização adequada das TIC em todos os processos organizacionais.

Segundo Ferreira *et al* (2001), CobiT encontra-se estruturado em quatro domínios:

- planeamento e organização que é a fase do planeamento estratégico das TIC de acordo com a estratégia da organização;

- aquisição e implementação, ou seja, após o planeamento identificam-se as soluções e procede-se a sua execução, controlando as mudanças que constantemente ocorrem;

- entrega e suporte, o objectivo aqui é fornecer serviços eficientes, mas é importante assegurar que o sistema continue a funcionar a um nível desejado e de forma contínua mesmo perante situações de desastre;

- monitorização e avaliação que consiste na verificação de todos os processos e na avaliação da adequação dos controlos internos.

Cada domínio é constituído por um conjunto de processos que auxiliam os gestores e auditores no controlo das TIC. Contudo convém aqui salientar que o CobiT não é uma solução pronta, devido a sua flexibilidade ele pode ser adaptado consoante as necessidades de cada organização, dependendo das actividades sobre as quais se pretende ter o controlo.

O CobiT apresenta inúmeras vantagens entre os quais ISACA destaca os seguintes:

- ajuda os gestores a alinhar os seus objectivos com os da organização;
- possibilita aos gestores uma visão mais alargada sobre o papel/importância das TIC;
- ajuda os gestores na aplicação das melhores práticas, através de um conjunto de ferramentas que auxiliam uma gestão mais flexível das TI;
- ajuda na redução dos riscos.

6.2 COSO

Segundo Cocurullo (2004) citado por Rego *et al* (s.d.) "o sistema C.O.S.O. auxilia na identificação dos objetivos essenciais do negócio de qualquer organização e define controle interno e seus componentes, fornecendo critérios a partir dos quais os sistemas de controle podem ser avaliados". Por seu lado, Pedro (2005) afirma que COSO é "um modelo de gestão de risco empresarial (…) que pode ser útil para o desenho e enquadramento da auditoria das tecnologias de informação e comunicação". Pode-se então afirmar que este é mais um método que fornece recomendações de como avaliar e melhorar os sistemas de controlo tendo por base a gestão dos riscos empresariais, podendo a organização estar mais capacitada para lidar com as incertezas e ter um sistema de informação mais fiável.

Para Rego *et al* (s.d) o modelo COSO define o controlo interno como sendo um processo, constituído por cinco sub-processos:

- ambiente de controlo (base para todos os outros componentes de controlo interno, fornece disciplina e estrutura);

- avaliação e gestão de risco (identificação e priorização dos riscos que podem por em causa o alcance dos objectivos pré-definidos);
- actividades de controlo (são as actividades que têm por objectivo a redução de riscos, quando executadas de forma adequada);
- comunicação e informação (a comunicação, podendo ser formal ou informal, constitui o fluxo de informação dentro da organização);
- monitorização (é a parte da avaliação e supervisão dos controlos); no fim de cada um desses cinco sub-processos deve-se proceder a uma avaliação dos mesmos.

Segundo Rego *et al* (s.d.) o modelo COSO apresenta a grande vantagem de oferecer uma solução ideal para o processo de gestão de riscos das organizações, já que este baseia na gestão de risco. Este modelo ultrapassa o enfoque tradicional que baseava na avaliação abrangente dos controlos e assenta numa auditoria baseada em riscos. Uma auditoria centrada em risco é mais eficaz que auditoria centrada apenas nos controlos, pois o auditor nesse caso pode direccionar o seu trabalho directamente para áreas de maior risco, em vez de identificar os controlos. A finalidade da auditoria baseada em riscos é o de antecipar e prevenir os riscos, ou seja, há todo um processo de levantamento da informação que permite o auditor identificar os riscos e as formas de mitigar tais riscos.

De acordo com Pedro (2005) “a gestão de risco empresarial permite aos gestores lidar eficazmente com a incerteza e risco associado, melhorando a capacidade de criar valor”. No entendimento de COSO o objectivo de qualquer entidade é criar valor, mas para isso está sujeito a riscos, porque existem as incertezas. A gestão de risco capacita uma organização a estar preparada para as incertezas.

6.3 ISO

ISO/IEC 17799 também denominado de Código de Boas Práticas para a Gestão da Segurança da Informação, segundo P.Silva *et al* (2003) definem por um padrão internacional, dedicado à segurança da informação, constituído por um conjunto de

orientações que visam contribuir para a definição e manutenção de um determinado nível de segurança das organizações, dos seus colaboradores, instalações e sistemas de informação.

Ferreira *et al* (2001) defendem que o ISO/IEC 17799 tem como objectivo permitir que organizações que cumprem a norma demonstrem publicamente que podem resguardar princípios, tais como a confidencialidade, integridade a disponibilidade das informações de seus clientes. Isto acontece através do estabelecimento de códigos de boas práticas para a gestão da segurança da informação e da disponibilização de instrumentos para a implementação de segurança da informação de acordo com características de cada empresa.

Para a concretização dos processos de gestão de segurança da informação, esta norma internacional, segundo P.Silva *et al* (2003) encontra-se organizada em dez capítulos com o objectivo de abarcar os diferentes tópicos ou áreas de segurança:

- Política de segurança;
- Segurança organizacional;
- Controlo e classificação de bens;
- Segurança do pessoal;
- Segurança física e ambiental;
- Gestão das comunicações e das operações;
- Controlo de acessos;
- Desenvolvimento e manutenção de sistemas;
- Gestão da continuidade do negócio;
- Conformidade.

Esta estrutura mostra a abrangência desta norma, o que significa que ela possui implicações na organização como um todo. Nota-se ainda que o ISO não aponta medidas específicas para cumprir os requisitos específicos de segurança, mas fornece uma base comum, ou seja,

oferece sugestões de segurança que apontam para níveis de segurança extremamente elevados, os quais devem ser adaptados às reais necessidades de cada organização.

Ferreira *et al* (2001) argumentam que esses dez capítulos são o resumo de cento e vinte e sete orientações de segurança que permitem identificar os controlos de segurança apropriados para a organização ou áreas de responsabilidade. Igualmente, estes autores referem a importância do ISO/IEC 17799 e afirmam que as suas orientações permitem ainda a uma organização construir de forma muito rápida uma política de segurança baseada em controlos de segurança eficientes, para além de permitir a conscientização sobre segurança para os funcionários, plano de continuidade dos negócios.

7 Considerações finais

Chegado a esta parte, pode-se afirmar que a auditoria resume num conjunto de procedimentos que permite verificar a aplicação e eficácia de controlos apropriados, ou seja, verificar se uma organização possui as práticas de segurança no seu sistema informático e se as mesmas estão em conformidade com as regras e procedimentos existentes na política de segurança da organização. Apesar da auditoria ser de grande importância no desempenho de um sistema informático, as actividades desta não devem ser excessivas para não interferir no funcionamento da organização.

Quanto a realização de uma auditoria, nota-se que ela pode ser interna ou externa. No primeiro caso é realizado por recursos da própria organização, no segundo caso a auditoria é realizada por auditores externos e que normalmente não têm nenhum vínculo com a organização auditada. Tanto a auditoria interna como a externa pode-se realizar, recorrendo a várias estratégias as quais destacam-se o questionário, a entrevista, *checklist*.

Em suma, pode-se afirmar que perante um mundo tecnológico cada vez mais complexo e dinâmico que se vive hoje, torna-se necessária uma mudança de cultura nas organizações, adoptando medidas de controlo que garantem a segurança do seu sistema informático. Surge daí a importância da prática da auditoria como meio fundamental para implementar controlos adequados por forma a acompanhar este dinamismo e reduzir os riscos a ele inerentes. Esta

prática é feita tendo por base vários padrões internacionais, os quais foram destacados neste estudo três desses padrões a saber: CobiT, COSO e ISO.

Capítulo 3: Segurança Informática nas escolas secundárias da cidade da Praia

1 Enquadramento

Este capítulo é o resultado daquilo que foi a parte empírica realizada nas escolas secundárias da cidade da Praia, tendo como propósito conhecer a realidade da segurança informática nestas escolas, ou seja, analisar e fazer uma avaliação das práticas da segurança informática levada a cabo nas mesmas.

No intuito de associar os conceitos sobre a segurança e auditoria informática e a sua aplicação prática, foi desenvolvida uma lista de aspectos a serem verificados junto das escolas secundárias da cidade da Praia. De ressaltar ainda que teve-se como suporte, por um lado, os vários aspectos que se devem ter em conta numa auditoria, como já foi aqui referido no capítulo anterior e, por outro, baseia-se num modelo apresentado pela ISO 17799 do qual seleccionou-se as que podem ser aplicadas a realidade das escolas secundárias.

Cumpre sublinhar, ainda, que perante esse propósito, continua-se com a firme convicção de que a metodologia que tinha-se delineado na parte introdutória deste trabalho, sobretudo no que toca aos métodos e técnicas de recolha de dados, é capaz de permitir obter dados importantes, objectivos e verificáveis.

2 Caracterização da amostra

Optou-se por uma amostra constituída pelas escolas secundárias da cidade da Praia. De um universo de 10 escolas secundárias, foram extraídos aleatoriamente 80%, para o efeito da aplicação da *checklist*. De referir ainda que a *checklist* foi aplicada aos responsáveis pela área de informática de cada escola.

3 Infra-estrutura das TIC

Compreender a estrutura das escolas em termos das tecnologias, ajuda a situar-se para melhor analisar os princípios de segurança informática vigentes nas mesmas. A tabela seguinte apresenta a caracterização da infra-estrutura tecnológica das escolas em estudo que, como se pode ver, estão representadas com a designação fictícia de letras alfabéticas.

	Escolas							
Designação	**A**	**B**	**C**	**D**	**E**	**F**	**G**	**H**
Número de computadores/estação de trabalho	50	78	45	50	55	45	50	40
Número de servidores	1	2	2	1	1	1	1	1
Número de router	1	1	2	2	1	2	2	1
Número de switch		5	2	2	1	2	2	1
Número de hub	5		1	1				2
Número de impressoras	3	5	3	4	2	3	4	2
Número de gerador		1		1	1			
Número de UPS	4	10	20	9	7	5	9	5
Número técnicos especializados na área das TIC	3	2	2	1	2	1	1	1
Escolas com ligações a internet	Todas							
As funções suportadas pelas TIC	Algumas							

Tabela 1- Infra-estrutura das TIC

Da análise da tabela 1, constata-se que o número de computador/posto de trabalho das instituições situa-se num intervalo de 40 a 78. A maioria dispõe de um único servidor e o número de *switch* e *router* varia entre 1 e 2 para ambos. Metade não tem *hub* e outra metade dispõe de 1, 2 ou 5. Todas as escolas têm 2 ou mais impressoras. Apenas 3 das escolas possui um gerador e todas possuem 4 ou mais UPS. O número de técnicos especializados na

área das TIC varia de 1 a 3 e apenas algumas funções das escolas são suportadas pelas TIC, enquanto que todas as escolas já dispõem de ligação a internet.

A infra-estrutura das TIC está relacionada com vários factores nomeadamente a dimensão das escolas, algumas com apenas uma sala de informática; as actividades que são suportadas pelas TIC, pois o que podemos verificar é que muita informação ainda encontra-se em formato analógico e muitas funções não passam pelas TIC, pois muitas das escolas ainda não dispõem de meios para o fazer. Um aspecto positivo a ser ressaltado é a disponibilização da internet em todas as escolas o que reveste num ganho significativo, não só para professores e alunos como uma poderosa ferramenta para pesquisas e estudo devido ao seu volume de informação disponível e à facilidade de acesso, possibilitando a construção do conhecimento mas também para a escola de um forma geral pela por disponibilizar a informação a qualquer momento, permitindo o contacto a distância com o mundo.

4 Apresentação dos resultados e a sua respectiva discussão e análise

Como se pode constatar no anexo a *checklist* encontra-se dividida nas seguintes partes: segurança física, lógica, de recursos humanos, política e plano de segurança, estrutura essa, que permitiria conhecer a realidade da segurança informática das escolas secundárias da cidade da Praia, pelo que passa-se de seguida a apresentar e analisar os resultados das informações recolhidas.

4.1 Segurança física

O primeiro ponto que questionou-se foi o controlo de acesso físico. Assim, começou-se por verificar se as escolas dispõem de mecanismos de controlo de acesso físico e ficou-se a saber que a totalidade delas possuem como mecanismo de controlo de acesso físico guardas nas entradas. Igualmente, como mecanismo de controlo de acesso dentro da organização, mais precisamente em locais onde estão instalados os equipamentos críticos, todas as escolas afirmam que são utilizadas apenas fechaduras nas portas, para impedir o acesso a pessoas

não autorizadas. Um aspecto que se verificou em quase todas as escolas é que as salas de informática tem portas gradeadas, reforçando assim a segurança física.

Contudo, o controlo de acesso físico não pode resumir-se apenas a guardas nas portas, mas apesar dos poucos recursos de muitas das escolas, nunca é demais reforçar a segurança com outros requisitos para aquelas escolas cujas condições lhe permitem, podendo optar por medidas adicionais para garantir o controlo de acesso tais como câmaras de vídeo-vigilância, leitor de cartões magnéticos, etc.

O que se pode dizer a esse respeito é que à entrada da organização o guarda deverá estar a tempo inteiro e, exigindo identificação sempre que uma pessoa deseja ter acesso à organização e que esta pessoa seja acompanhada dentro da organização por alguém responsável por este serviço.

Referente a segurança dos equipamentos a totalidade das escolas defende que estes estão localizados em zonas seguras, ou seja, as salas dos computadores e demais equipamentos são de acesso apenas a pessoas autorizadas e quando não estão sendo utilizadas, as portas destas instalações são sempre fechadas em segurança.

Entretanto, perguntado se estão definidos os requisitos de segurança das condições ambientais, ou seja, se existe monitorização das condições ambientais para proteger os equipamentos do calor, humidade, poeira, entre outros aspectos que possam prejudicar o bom funcionamento dos equipamentos, apenas 25% afirmam que existem essas condições, enquanto que 75% afirmam que não, como se pode ver no gráfico que se segue.

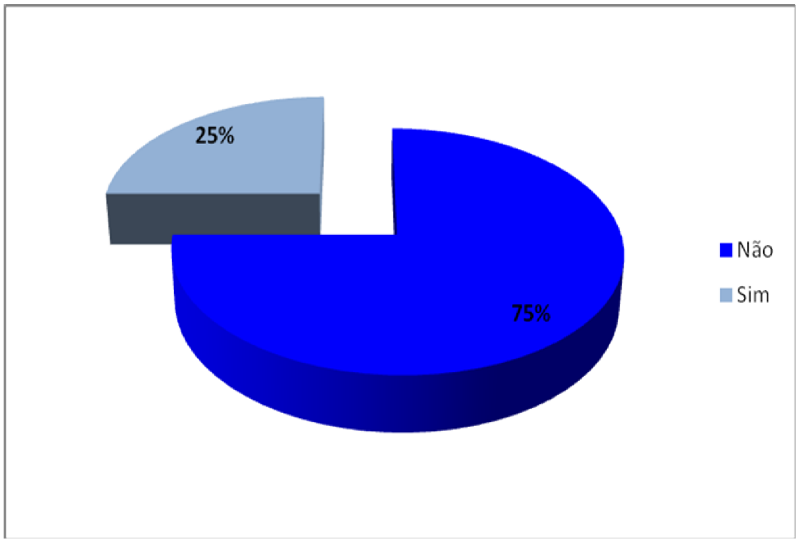

Gráfico 1 – Monitorização das condições ambientais

O que se pode notar é que a instalação dos equipamentos, muitas vezes, é feita de acordo com as condições físicas de cada instituição, relegando as questões de segurança para o segundo plano. Contudo, as salas onde estão alojados os equipamentos devem estar climatizadas, com ar condicionado, arejamento, existindo assim condições para impedir a poeira, a humidade ou outro factor que possa causar algum dano nos equipamentos.

Quis-se saber se existe um controlo adicional de segurança para os equipamentos críticos, em situações de emergência tais como incêndio, inundação, etc, e teve-se a oportunidade de verificar que todas as escolas dispõem extintores para protecção contra incêndio, contudo como nos ilustra o gráfico seguinte, em 75% das escolas não são efectuados testes regularmente nos equipamentos de emergência, o que constitui a nosso ver um aspecto que carece de melhorias, pois assim como adquirir equipamentos, é igualmente necessário habilitar os colaboradores de conhecimentos necessários para a sua correcta utilização.

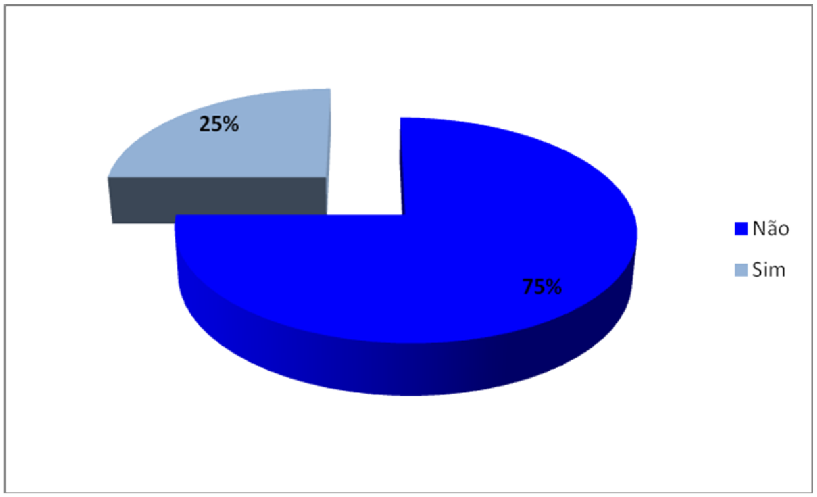

Gráfico 2 – Realização de testes nos equipamentos de emergência

Para casos de falhas de energia, é importante que as escolas estejam munidas de equipamentos que impeçam a indisponibilidade dos seus serviços críticos. Para isso, questionou-se aos responsáveis informáticos nas escolas da existência de geradores e de sistemas UPS, pelo que ficou-se a saber que 63% delas não dispõem de um gerador, mas em contrapartida grande parte, 87% das escolas, dispõem de um sistema UPS nos seus equipamentos, como dão conta os gráficos seguintes.

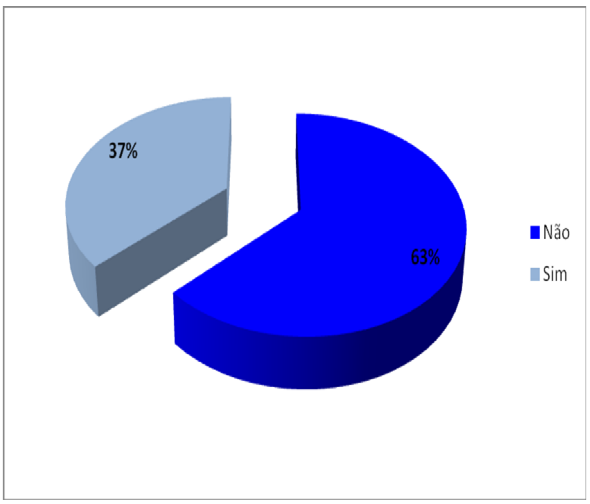

Gráfico 3 – Existência de geradores

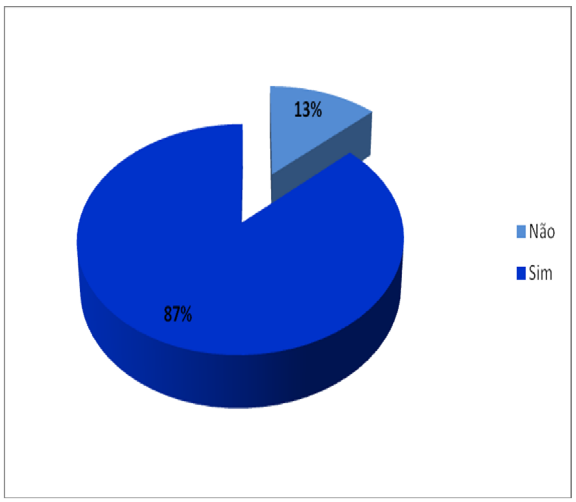

Gráfico 4 – Existência de sistema UPS

No que toca a manutenção dos equipamentos, os dados nos mostram que na totalidade das escolas a manutenção dos equipamentos é feita por técnicos especializados, contudo não

existem formas de registar falhas nos equipamentos (63%), de modo a que, por um lado, os futuros problemas sejam mais facilmente resolvidos e, por outro, facilitar o trabalho de posteriores pessoas que vierem a fazer o mesmo trabalho.

Apenas 12% das escolas dispõem de um serviço *Help Desck*, conforme nos mostra o gráfico que se segue (de referir que esta percentagem refere à escola em que a NOSI – Núcleo Operacional da Sociedade de Informação – começou a informatizar os seus serviços e que por isso, qualquer problema que tenha alguma ligação com as tecnologias é reportado para a NOSi para a sua respectiva resolução). Entre as inúmeras vantagens de um centro *Help* Desck pode-se destacar o suporte, no momento exacto, em caso de qualquer problema técnico, evitando, entre outros, pôr em causa o princípio da indisponibilidade.

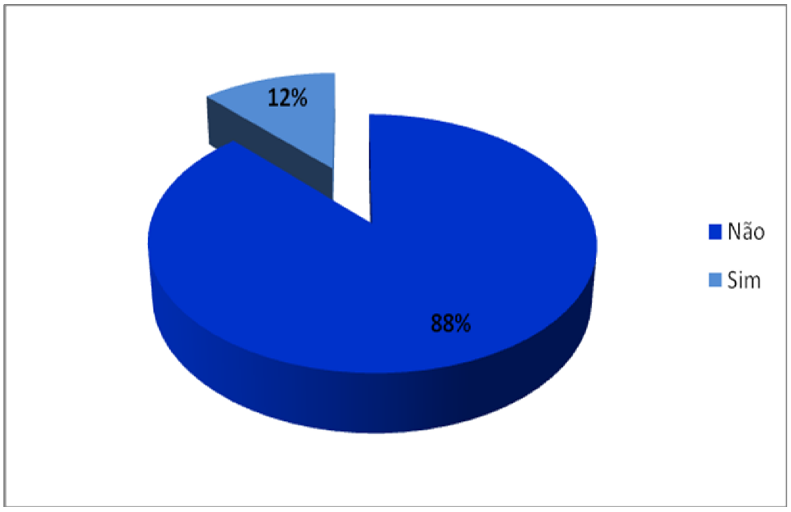

Gráfico 5 – Existência de um centro *Help Desck*

4.2 Segurança lógica

Apesar de grande parte das escolas (75 %) afirmarem ter já definidas as exigências respeitantes ao controlo de acesso lógico, mais precisamente as restrições e permissões de acesso a serviços e a definição de *password* para cada utilizador, quase nenhuma delas (25 %) preocupa em documentar tais regras, conforme apresenta os seguintes gráficos.

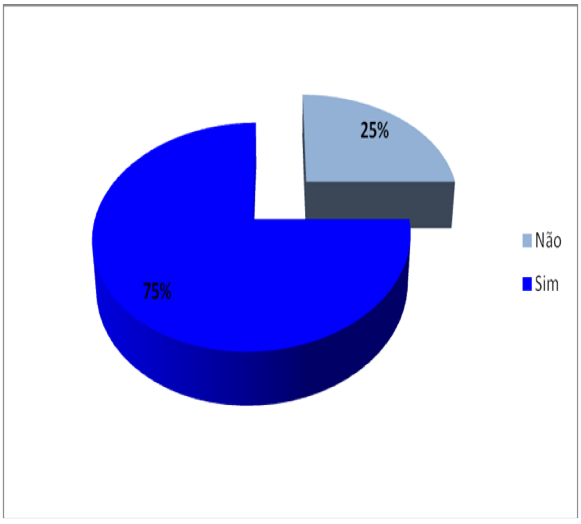

Gráfico 6 - Definição das exigências de controlo de acesso lógico

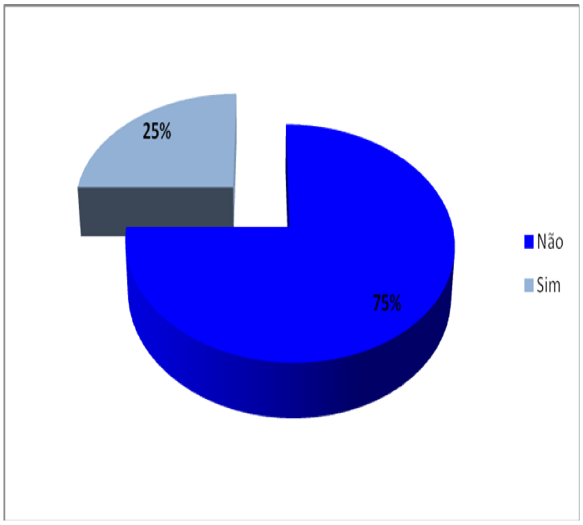

Gráfico 7 – Estas exigências encontram-se documentadas

Grande parte das escolas (75%) alega que não existem requisitos de segurança em caso de utilização de sistemas novos, como por exemplo ter oportunidades de teste isolado dos procedimentos operacionais, segundo consta no gráfico que a seguir se apresenta.

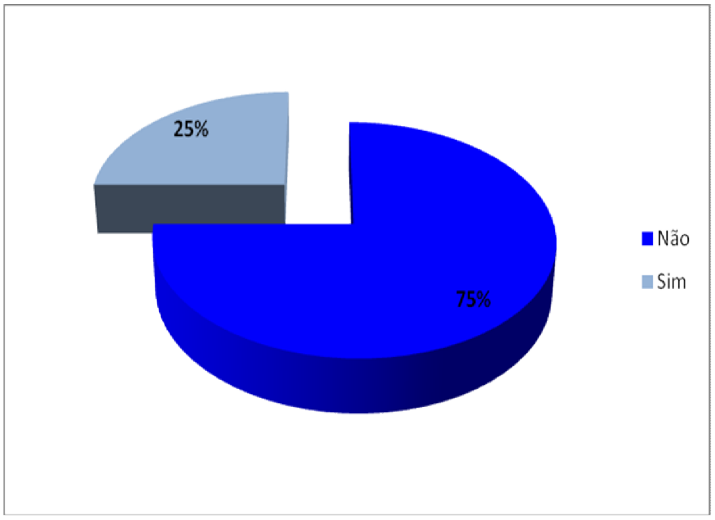

Gráfico 8 – Existência requisitos de segurança em casos de utilização de sistemas novos

Questionado se existe alguma auditoria interna para verificar se existe utilização de *software* não autorizado, a totalidade dos entrevistados alegam que não e ainda, como argumentam por falta de recurso, os *softwares* utilizados não são licenciados, o que implica maior vulnerabilidade para um sistema, em termos, por exemplo, de actualizações.

Outro aspecto que verificou-se e que reveste de grande importância na segurança de um sistema informático de qualquer organização refere-se a actualização dos sistemas. Conforme mostra o gráfico que se segue, a maioria das escolas (75%) afirma que os seus sistemas estão sujeitos a actualizações, o que constitui um aspecto positivo pois, a não actualização dos sistemas é que os torna vulneráveis e sujeitos a diferentes tipos de ataques.

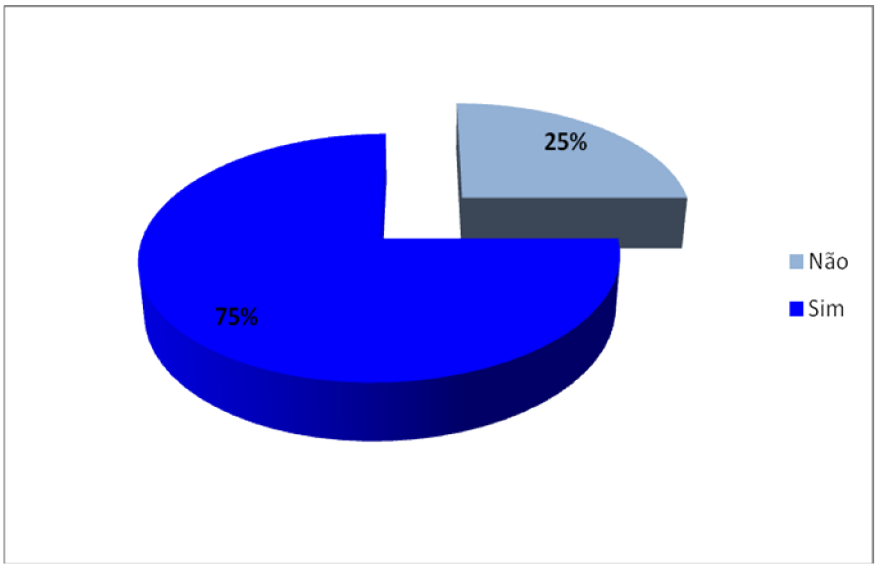

Gráfico 9 - Os sistemas estão sujeitos a actualizações

Para a totalidade das instituições em estudo, existe um sistema antivírus actualizado, mas em nenhuma dessas este sistema antivírus é centralizado. A existência de um *software* antivírus actualizado para prevenir a entrada de vírus no ambiente computacional, constitui um aspecto positivo a ressaltar, se levar em consideração que a propagação de vírus constitui, sem dúvida, uma das grandes ameaças a um sistema informático. Entretanto, para além de actualizado, se este sistema for também centralizado, permitirá um melhor controlo, podendo a actualização ser feita de forma automática, a partir de um ponto único.

Apenas 12% das escolas afirmam que realizam cópias de segurança, segundo consta no gráfico que se segue, contudo não existem especificações explícitas para o efeito, ou seja, não existe nenhuma especificação formal sobre o que é que deve ser copiado, quando e quem deve realizar essas cópias. De referir que ter um sistema de *backup* funcional e completo de toda a informação da organização seria a medida mais adequada, mas devido as exigências e aos custos que este acarreta, nesse caso aquelas escolas em que os recursos não permitem, poderiam optar por uma cópia de segurança parcial. Por outras palavras, seria aconselhável

que adoptassem procedimentos simples nomeadamente seleccionar a informação necessária para efeito de cópias de segurança que ficava guardada num disco externo, por exemplo, ou outro local seguro.

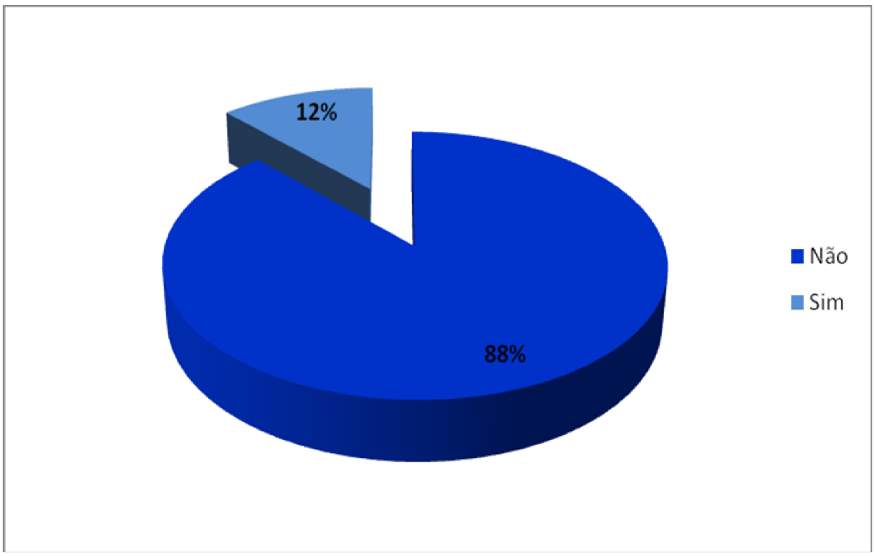

Gráfico 10 – Realização das cópias de segurança

Quanto a segurança da rede informática, metade das escolas, afirma que ainda não dispõe de uma política de segurança de rede informática e os equipamentos da rede ainda não estão devidamente identificados com o nome, endereço, localização e utilizador de cada equipamento. Isso é importante porque por exemplo quando existe um computador na rede com algum vírus, ou se algum utilizador está a praticar algum acto ilícito, os mecanismos de controlo permitem identificar exactamente qual é o computador e onde está localizado.

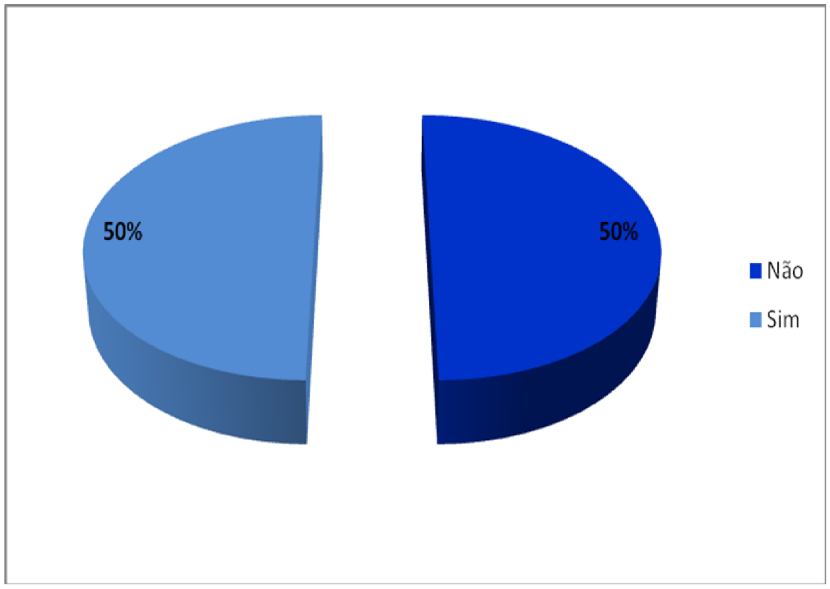

Gráfico 11 - Existe uma política de segurança de controlo de acesso a rede

Quanto a utilização da internet, a totalidade das escolas afirma ter ligação internet ao seu sistema informático, mas ao mesmo tempo, a maioria delas (75%) afirma que ainda não têm definido os requisitos de segurança para a utilização da mesma. Se considerar a internet a principal porta para entrada de vírus ou outros *softwares* maliciosos num sistema, esta deveria ser uma questão a ter em conta nas melhorias a serem implementadas.

Os dados mostram ainda que 63% das escolas ainda não dispõem de um *firewall* ou um servidor *proxy* para ditar as permissões e restrições na utilização da internet nomeadamente referente a conteúdos ou *sites* a serem utilizados e consequentemente, não realizam actualizações na lista negra (lista dos sites ou conteúdos definidos como os que não podem ser acedidos dentro da rede da organização).

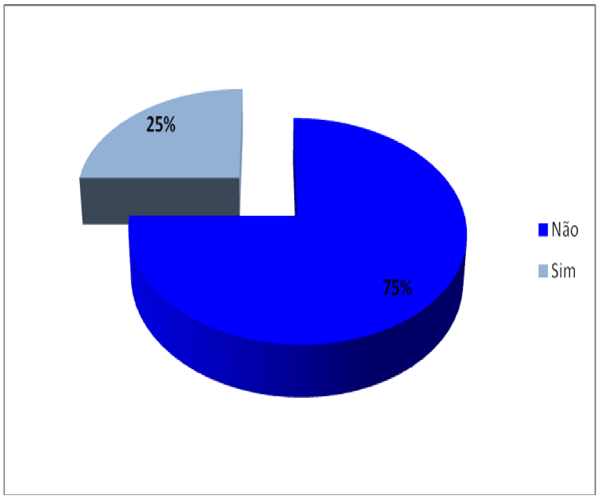

Gráfico 12 - Definição dos requisitos para a utilização da internet

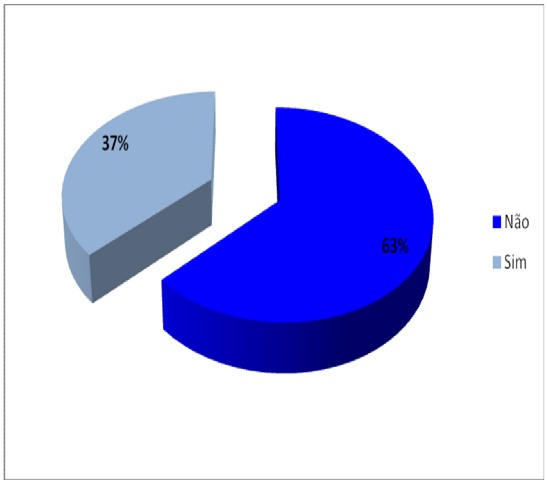

Gráfico 13 - Existe um *firewall* ou um servidor *proxy*

4.3 Segurança de recursos humanos

Os dados recolhidos mostram que nenhuma das escolas abordadas dispõe de programas de formação ou alguma campanha de sensibilização relativamente a questões de segurança informática. Convém aqui sublinhar a importância de programas de formação/sensibilização dos recursos humanos para questões de segurança informática, pois são eles que interagem directamente com as TIC no seu dia-a-dia e, por isso, deverão estar informados/sensibilizados como realizar tarefas quotidianas sem pôr em causa a segurança do sistema. A componente humana sem a devida formação, nesse caso, pode constituir uma ameaça para o sistema podendo ter como consequências, por exemplo, a indisponibilidade dos serviços, perda de algum dado relevante, entre outros.

Um exemplo dos aspectos a ser informado aos colaboradores, é a utilização segura de *password*, que como teve-se oportunidade de ver mais acima, apesar estarem definidos os requisitos para a utilização de *password*, na prática isto não é uma realidade, pelo que 75% das escolas afirmam que as regras para a utilização segura de *password* não são tidas em consideração no dia-a-dia dos utilizadores, como se pode constatar no gráfico que se segue.

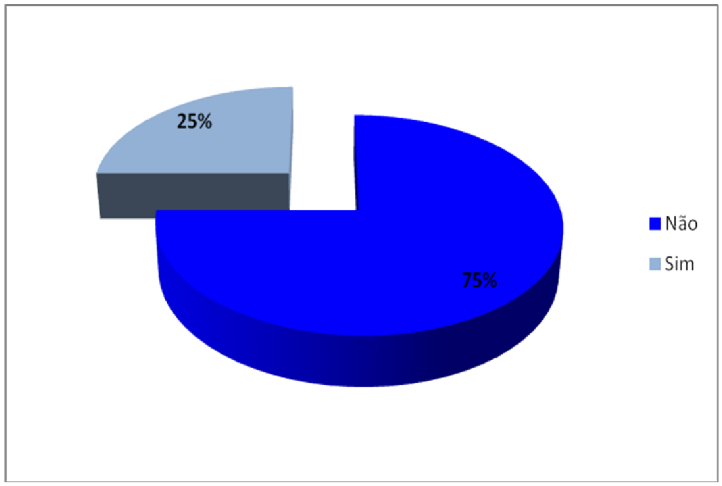

Gráfico 14 - Utilização segura de *password*

Quis-se também saber sobre a utilização dos equipamentos, ao que constatou-se que em nenhuma das escolas existe a preocupação de sensibilizar os utilizadores para uma utilização segura dos equipamentos.

Um outro aspecto que verificou-se relacionado com a segurança dos recursos humanos tem a ver com a contratação e saída de recursos humanos da organização. No que diz respeito a segurança referente ao recrutamento e saída de colaboradores da organização, as informações recolhidas mostram que nenhuma das escolas especifica os requisitos para o recrutamento de novos colaboradores. Quanto a segurança quando um colaborador abandona a organização, apenas 25% das escolas afirmam que são cessadas todas as permissões quando um colaborador abandona a organização. Particularmente para funções sensíveis faz-se necessário que o processo de segurança começa desde o momento de recrutamento de um novo colaborador, fazendo o seu enquadramento através da divulgação das regras de segurança existentes e, cessando as suas permissões quando este abandona a organização.

4.4 Política e plano de segurança

Questionado sobre a existência de um plano de segurança, a totalidade das escolas afirma que não existe nenhum plano de segurança definido. Igualmente, em nenhuma das escolas existe uma política de segurança, ou qualquer outro documento escrito que contenha normas e regras respeitantes às práticas de segurança existentes.

Neste contexto, pode-se dizer que é necessário que sejam introduzidas melhorias, a definição de uma política e de um plano de segurança são documentos fundamentais para a implementação da segurança nas organizações. A política de segurança como documento que contem todas as regras, normas e princípios que visam manter a segurança numa organização, bem como as respectivas sanções em caso de violação dos mesmos, permite clarificar os objectivos da organização e orienta a sua actuação em matéria de segurança.

O plano de segurança, por seu lado, é também importante porque permite uma organização estar capacitada para reagir perante situações imprevisíveis que podem ocorrer e que podem interromper o normal funcionamento desta. Uma organização com um plano de segurança definido funciona num ambiente de maior confiança, isto é, estão criadas as condições para o exercício das suas actividades críticas face a ocorrências de situações de desastre.

5 Síntese/apreciação global dos resultados

Da apreciação global dos resultados pode-se dizer que se, por um lado, já se pode falar em algumas exigências relativamente a questões de segurança informática nas escolas, tais como o controlo de acesso físico, controlo de acesso lógico, actualização dos sistemas, existência de um sistema antivírus, por outro, depara-se com aspectos importantes de segurança que ainda não se encontram definidos. Está-se a referir, particularmente a segurança dos recursos humanos e a definição de plano e política de segurança ou qualquer outro documento formal onde constam as regras de segurança.

Especificamente a segurança dos recursos humanos os resultados mostram que nenhuma escola em estudo definiu ainda os princípios de segurança. Relembra-se aqui que os recursos humanos assumem um papel importante na definição e implementação da segurança numa organização, considerando que grande parte dos danos nos sistemas provêm de erros humanos causados muitas vezes por falta de uma formação específica em matéria de segurança, esta deveria ser um aspecto a ser tido em conta.

De igual modo, a definição de um plano de segurança, reveste-se de grande importância por permitir à organização a continuidade dos seus serviços face a situações de desastre.

Um outro aspecto igualmente importante e que ainda não é uma realidade em nenhuma das escolas é a definição de uma política de segurança. Assim, deverá estar devidamente formalizado num documento escrito as regras, normas e princípios de segurança, deverão também estar presente as sanções. Este documento denominado de política de segurança deve ser praticável e eficaz, aprovada pela gerência, publicada e comunicada a todos os colaboradores e sujeita a revisões periódicas conforme as mudanças vão ocorrendo.

Dada a importância deste documento e para que sejam mantidos os aspectos positivos já identificados e melhorar os menos conseguidos, decidiu-se em jeito de proposta de melhoramento, definir uma política de segurança para as escolas secundárias da cidade da Praia, que possa servir de *input* na procura de melhores soluções na implementação da segurança informática. O que se pretende é propor um modelo aberto e flexível, que pode ser adaptado a realidade de cada escola.

Convém referir que para o desenvolvimento deste modelo de política de segurança teve-se como referência a norma ISO 17799 pois, como foi anteriormente referido esta norma é o código de prática para a gestão da segurança da informação e, ainda teve-se em consideração as informações recolhidas, ou seja, a realidade das escolas secundárias da cidade da Praia. Teve-se ainda como referencia o modelo de política de segurança apresentado por Spanceski (2004) para uma instituição de ensino.

É importante também ressaltar que quando se define uma política de segurança para instituições de ensino deve-se levar em conta que existe a particularidade de ser constituída não só pelos funcionários que trabalham na organização como também pelos alunos que assistem a aulas e que de certa forma utilizam os recursos tecnológicos da organização e têm acesso a informações da organização e que, por isso, também devem estar cientes das suas responsabilidades e da importância da segurança informática.

6 Proposta de melhoramento

Dada a inexistência de uma política de segurança nas escolas em estudo e como forma de definir a segurança informática nas mesmas, a proposta vai no sentido de apresentar uma política de segurança baseada na norma da ISO/IEC 17799.

6.1 Proposta de Política de Segurança para as escolas secundárias da cidade da Praia

6.1.1 Enquadramento

A política de segurança é a expressão que formaliza todas as regras, normas e procedimentos relacionados com todos os aspectos que envolvem a segurança informática de uma organização. Para além de garantir que existam controlos apropriados de segurança, permite igualmente definir as acções previstas em caso de violação da política.

6.1.2 Objectivos da Política de Segurança

Pretende-se com esta política definir as responsabilidades e direitos dos utilizadores, definindo as atribuições de cada um, ou seja, o que pode ou não ser feito em relação aos requisitos de segurança informática da organização. A política permite assim, assegurar a qualidade nos serviços, com base em comportamentos profissionais de todos os colaboradores, evitando falhas de segurança.

Para que tais objectivos sejam realidade, é fundamental que a política de segurança considere alguns requisitos nomeadamente: ser apresentada de forma clara e concisa para ser de fácil entendimento por todos; ser do conhecimento e da concordância de todos os utilizadores; estar disponível para todos na organização. Tudo isso no sentido de todos os utilizadores dos recursos tecnológicos sintam envolvidos e sensibilizados para questões da segurança informática. As normas descritas nesta política devem estar sujeitas a actualizações conforme as mudanças que ocorrem na organização.

A política de segurança será dividida em três pontos principais a saber políticas de segurança física, lógica e de recursos humanos, sendo estes subdivididos em tópicos. Tendo em conta que se trata de uma política para instituições de ensino em que os actores têm papéis bem distintos, convém referir que algumas das regras que não têm carácter geral serão especificadas para alunos e para os restantes funcionários.

6.1.3 Política de segurança física

O Objectivo deste tópico é prevenir o acesso não autorizado, dano e interferência às instalações físicas da organização e à sua informação (ISO 17799).

6.1.3.1 Controlo de acesso

Regras gerais

- O acesso à organização deve ser controlado por guardas que devem exigir identificação das pessoas na porta.
- Os terceiros que prestam serviços deverão igualmente, utilizar alguma forma identificação.
- Pessoas que não pertencem à organização devem ser acompanhadas dentro da organização.
- As portas e janelas que dão acesso à organização deverão ser mantidas fechadas em segurança quando não utilizadas.
- Apenas pessoas autorizadas devem ter acesso a salas onde encontram informações confidenciais tais como informações financeiras e académicas dos alunos ou outra documentação dos funcionários ou qualquer outra informação que reveste de carácter sigiloso para a organização.
- O acesso aos laboratórios de informática deve ser controlado, sendo a sua utilização permitida mediante a supervisão de um funcionário responsável para o efeito.
- A segurança e a ordem dos laboratórios de informática é da inteira responsabilidade dos professores, durante o tempo em que estes utilizam os mesmos.
- As salas onde estão instalados os recursos tecnológicos devem estar fechadas e em segurança quando deixados sem supervisão.

- Deverá existir uma sala específica para servidores, estas salas devem permanecer fechadas e com acesso livre apenas ao pessoal autorizado e devem estar devidamente climatizadas.

- A sala de servidor deverá possuir um sistema de detecção/alarme e combate automático para caso de incêndio.

- Devem ser realizadas cópias de segurança, estas deverão ser realizadas pelo responsável pela segurança e ter periodicidade variável, conforme vão surgindo informações que se considerem relevante para a organização, contudo no fim de cada trimestre deverá haver um *backup* completo das informações previamente seleccionadas.

6.1.3.2 Manutenção/utilização dos equipamentos

Regras gerais

- Os utilizadores devem estar informados sobre a correcta utilização dos equipamentos.

- O suporte e manutenção de equipamentos informáticos só poderão ser prestados por técnicos especializados na área, deverá existir uma equipa técnica interna ou prestadora de serviços disponível para eventuais necessidades.

- As falhas nos equipamentos devem ser registadas em lugar (analógico ou digital) específico para tal, para uma mais rápida resolução de falhas semelhantes que vierem a surgir posteriormente e para facilitar o trabalho a outras pessoas que vierem a fazer o mesmo trabalho.

- Deverá existir um centro/serviço *Help Desk*, para uma melhor e mais eficiente gestão dos problemas nos equipamentos.

- Os equipamentos devem ser protegidos contra falhas de energia e outras anomalias na alimentação eléctrica utilizando-se para além de UPS, também geradores evitando a indisponibilidade dos serviços.

- Todas as salas deverão possuir extintores para combate a incêndio.

- Deverá existir monitorização das condições ambientais (protecção contra humidade, calor, poeira, ou outro factor que possa causar dano nos equipamentos) nas salas onde se encontram recursos tecnológicos particularmente nos que guardam informações críticas.

6.1.4 *Politica de segurança lógica*

Pretende-se com este ponto especificar algumas regras, que consideram-se fundamentais para reduzir os riscos relacionados com a segurança lógica.

6.1.4.1 Politicas de utilização de antivírus

Regras gerais

- Deverá existir um sistema antivírus que seja actualizado e centralizado.
- A actualização do antivírus deverá ser feita também de forma automática e centralizada a todos os computadores da rede.

6.1.4.2 Políticas de utilização de password

Regras gerais

- As *password* deverão conter no mínimo oito caracteres entre letras maiúsculas e minúsculas, caracteres especiais e números.
- Na criação de *password* deve-se evitar o uso de informações pessoais, tais como nomes de familiares, de cidade, números de telefone, datas ou outros que poderiam ser facilmente descobertos.
- Deve-se evitar anotar a *password* em papel ou em outros meios de fácil acesso, para isso deve-se utilizar um método próprio para lembrar da *password*, de modo que ela não precise ser escrita em nenhum local.
- As *password* não deverão ser compartilhadas visando proteger as informações do acesso de pessoas não autorizadas.

6.1.4.3 Política de utilização da rede

Regras gerais

- Por uma questão de segurança deverão existir dois domínios: o domínio GERAL que deve constar as contas dos professores e alunos (estes utilizam serviços como aulas e internet) e o domínio SERVIÇOS onde constam as contas dos demais funcionários (estes utilizam as aplicações definidas pela empresa e prestam serviços internos à organização tais como contabilidade, gestão de recursos humanos, entre outros).

- O acesso ao sistema informático da organização, deve ser controlado pela identificação do utilizador, ou seja, cada utilizador deve estar devidamente autenticado através da utilização de uma *password*.

- Durante a ausência do utilizador, o computador deve permanecer bloqueado, ou seja, após algum tempo de inactividade ou ao se ausentar do local de trabalho o utilizador deve fazer o *logoff* ou bloquear o computador, protegendo a rede contra acessos não autorizados.

- A utilização de equipamentos de informática particulares tais como portáteis com acesso a rede deve ser do consentimento do departamento da tecnologia estes equipamentos devem estar registados no domínio (GERAL) e configurados de acordo com os requisitos de segurança vigentes na organização.

- Os direitos de acesso dentro da rede devem ser definidos em conformidade com as actividades que cada um desempenha na organização.

- Não são permitidas atitudes/acções tais como tentativas de acesso não autorizado a dados ou a conta de outro utilizador; tentativas de invadir ou sobrecarregar/congestionar deliberadamente a rede; tentativas de invadir o servidor; igualmente não são permitidas alterações de configurações de rede, por pessoas não autorizadas, entre outros que pode pôr em causa o normal funcionamento da rede.

- Documentos cujo conteúdo não têm nenhuma ligação com os objectivos da organização, nomeadamente os de natureza pornográfica, não devem ser gravados através do uso de recursos computacionais da rede, evitando assim sobrecarregar a conta com conteúdos desnecessários.

- O acesso remoto (o tráfego de informações) deverá ser protegido por VPN, quando se trata de informações confidenciais e críticas para a organização.

- Deverá ser instalado na rede um *software* para detecção de intrusos (IDS) para identificação de qualquer tipo de intrusão que possa prejudicar o normal funcionamento do sistema.

- As redes de computadores deverão ser protegidas por um *firewall* que esteja operacional, devidamente configurado e permanentemente actualizado, igualmente qualquer tráfego que vem da rede externa deverá passar pela DMZ.

- Deverá ser garantida e protegida toda infra-estrutura da rede da organização com intuito de proteger consequentemente as informações que nela trafega, do mesmo modo, os serviços que não são necessários ao funcionamento da organização não devem estar a correr nos servidores.

- Deverá ser definido um plano de contingência (com operacionalidade prática) a fim de possibilitar a continuidade dos serviços em caso de algum sinistro.

6.1.4.4 Administração de contas

Regras gerais

- Documentos dos alunos bem como documentos pessoais dos funcionários não estão sujeitos a cópias de segurança, daí que cada um deve fazer cópias dos documentos que considere necessário.

- A manutenção dos arquivos na conta pessoal é de responsabilidade do utilizador, sendo que o mesmo deve evitar cúmulo de arquivos desnecessários, sendo assim, a escola não se responsabiliza por qualquer documento dentro das contas pessoais dos utilizadores do domínio GERAL.

- Não é feita cópia de segurança dos arquivos do domínio GERAL.

- O utilizador será automaticamente desconectado se ficar sem usar o sistema por mais de 30 minutos para evitar o uso do mesmo por outro utilizador que poderá estar mal intencionado quanto ao acesso e consulta das informações.

- O responsável de segurança tem o direito de desactivar/bloquear a conta do utilizador, seja ele aluno e/ou funcionário, sempre que esteja perante situações de quebra de segurança, ou seja, face a prática de actos que ponham em causa a segurança da organização ou acede a dados dos outros sem autorização, entre outros.

Regras para funcionários:

- Todo o funcionário deve ter uma conta particular de acesso aos recursos da rede e demais recursos com as respectivas permissões e restrições previamente definidas.

- A desactivação das contas acontece em casos de não utilização por um período de mais de um mês para os funcionários.

- Cada funcionário deve ter no servidor uma pasta onde guarda seus arquivos que devem ser sujeitos a possíveis cópias de segurança.

Regras para alunos:

- Todo o aluno, após a efectivação da sua matrícula, deve ter uma conta particular de acesso aos recursos a que está autorizado e lhe será atribuído uma *password* que pode ser alterada desde que este respeite as regras da criação da *password* estipuladas pela organização.

- A desactivação das contas acontece em casos de não utilização por um período de mais de um trimestre.

6.1.4.5 Política de utilização da internet

Regras gerais

- Os servidores devem possuir mecanismos de protecção contra vírus e códigos maliciosos.

- Deve-se evitar executar ou abrir e-mail com arquivos anexados enviados por remetentes desconhecidos ou suspeitos, que de alguma forma pode perturbar o normal funcionamento das actividades da organização.

- Não é permitido o acesso a sites com conteúdo pornográfico, jogos, bate-papo, serviços tais como Rádios On- Line, e outros afins; caso julgue necessário estes serão bloqueados. O ideal é que cada utilizador tenha acesso apenas aos serviços necessários para o desempenho das suas funções.

- Será proibida a abertura de arquivos executáveis (arquivos com extensão .exe por exemplo) recebidos por e-mail, evitando assim a propagação de vírus pela rede.

6.1.4.6 Segurança da informação

Regras gerais

- Toda a informação deve ser protegida contra acesso, alteração, destruição, quer seja acidental ou intencional.

- A definição do acesso a informação deve estar ligada a posição que a pessoa ocupa na organização.

- Toda informação que se considere necessário, deve ser guardado no servidor com as devidas condições de segurança.

- Devem existir as condições de recuperação da informação, por isso, as cópias de segurança deverão ser guardadas em locais seguros.

- Para proteger da utilização de *softwares* piratas e de vírus ou problemas técnicos, o utilizador está proibido de instalar ou remover *softwares* salvo em casos que é devidamente acompanhado e autorizado por alguém da equipa técnica.

- O uso de qualquer equipamento para o processamento das informações fora dos limites físicos da organização (como por exemplo uso de portáteis em casa) deverá ser autorizado pelo responsável da segurança e perante as devidas condições de segurança.

6.1.5 *Segurança dos recursos humanos*

Regras gerais

- Os funcionários devem comprometer através de um documento escrito a preservar o sigilo das informações da organização.

- Todos os utilizadores dos recursos tecnológicos da organização deverão receber acções de formação/sensibilização nos procedimentos de segurança e no uso correcto dos equipamentos.

- Todos os utilizadores devem estar conscientes da possibilidade de ocorrência de incidentes como ameaças, falhas que possam ter impacto no funcionamento das actividades da organização.

- Todas a regras e procedimentos de segurança devem ser documentados e divulgados a todos os utilizadores que beneficiam do uso do sistema.

- O responsável de segurança deverá supervisionar todos os utilizadores, certificando-se do uso e implementação de regras básicas de segurança, com especial atenção para os colaboradores novos ou inexperientes.

- A equipa responsável pela segurança deverá ser formada pelo menos por duas pessoas para evitar problemas como a indisponibilidade de serviços em casos de ausência de uma pessoa.

- Deverá ser estabelecido um processo disciplinar formal para fazer face a violação de políticas e procedimentos de segurança existentes na organização.

- A demissão de um funcionário deve ser acompanhada pela desactivação de todos os acessos deste utilizador a qualquer recurso da organização, para evitar posterior acesso a informações da organização.

6.1.6 *Aplicabilidade*

Esta política de segurança se aplica a todos os alunos, professores, restantes funcionários e prestadores de serviços que tenham acesso às instalações das escolas. Sendo assim cabe ao responsável pela segurança zelar pelo cumprimento de regras e princípios estipulados, o que não isenta cada utilizador em particular da responsabilidade das regras estabelecidas na política a que lhe diz respeito.

6.1.7 *Sanções*

O não cumprimento das regras da política de segurança não pode ser justificado pelo desconhecimento do mesmo, pois este deve ser do conhecimento e entendimento geral. É importante que após a detecção de violação das normas de segurança estabelecidas na política de segurança, determinar se a violação foi causada de forma intencional ou não. Aos utilizadores que, de forma não intencional desrespeitarem as normas de segurança estabelecidas nesta política de segurança serão aplicadas as seguintes sanções: advertência verbal, comunicando a norma que foi violada e em último caso, será bloqueado o acesso ao sistema da organização. Aos utilizadores que de forma intencional violarem as regras de política de segurança, ficam automaticamente bloqueado o acesso ao sistema da organização serão aplicadas as seguintes sanções: advertência escrita, e em último caso, a demissão.

Conclusão

Chegado a esta parte, está-se em condições de tecer algumas conclusões sobre este trabalho. Os resultados deste trabalho permitem compreender os principais conceitos e técnicas de segurança e auditoria informática e conhecer a realidade da segurança informática nas escolas secundárias da cidade a Praia. Quanto a isso pode-se afirmar que, apesar de ainda faltar muito para se fazer, existe já uma consciência, por parte dos responsáveis pela área, que investir em segurança passou a ser uma necessidade para qualquer organização que nas suas actividades do dia-a-dia lida com tecnologias de informação.

O sistema informático das escolas em estudo, como qualquer outro, tem as suas vulnerabilidades, mas não obstante alegarem falta de recurso, que leva a limitar a potencialidade técnica para detectar e explorar vulnerabilidades, defendem que a segurança deve constar entre as questões prioritárias da definição de políticas e funcionamento de uma organização. Quanto a isso pode-se afirmar que, apesar de não ser possível ter um sistema completamente seguro, muito se pode fazer para reduzir ao mínimo a ocorrência de ataques. Para que isso aconteça, uma atitude coerente seria apostar em medidas preventivas, ou seja, criar as condições para conhecer as próprias vulnerabilidades e corrigi-las antes de serem exploradas por utilizadores não autorizados, pois as ameaças só acontecem perante ocorrência de vulnerabilidades.

Algumas medidas de segurança informática já são realidade nas escolas nomeadamente o controlo de acesso, política de actualização e sistema antivírus, entretanto muitos outros

aspectos considerados importantes ainda estão por definir, está-se a referir particularmente a definição de planos e de uma política de segurança.

Pode-se constatar que ainda não existem acções de formação ou de sensibilização dos recursos humanos para questões de segurança. Nesse particular, pode-se reforçar que quanto mais capacitados forem os colaboradores para ter uma visão e postura crítica perante aspectos de segurança, mais sucesso obterá a organização na implementação das suas medidas e políticas de segurança, tendo em conta que são esses que lidam directamente com as tecnologias.

Dos resultados obtidos do trabalho prático, sentiu-se a necessidade de propor uma política de segurança. Isso justifica-se por ter-se constatado que em nenhuma das escolas existir esse documento formal e por considerar que tal documento constitui um dos pontos fundamentais e básicos para se implementar a segurança em qualquer organização. O propósito foi propor um modelo flexível, capaz de adaptar à realidade (como o ambiente, a estrutura, os recursos disponíveis) de cada uma das escolas.

No que toca à metodologia adoptada, pode-se afirmar que permitiu chegar aos resultados pretendidos. O que pode-se constatar é que, se por um lado, conseguiu-se inteirar dos conceitos e das técnicas de segurança e auditoria informática, por outro, conseguiu-se fazer a ponte entre a teoria e a prática, verificando a aplicabilidade desses conceitos e técnicas nas escolas que foram o objecto de estudo.

Essas conclusões permitem, com efeito, afirmar que urge uma mudança de mentalidades em que as tecnologias de informação e comunicação passam a ser vistos como recursos estratégicos e críticos, pois cada vez mais a sobrevivência das organizações depende delas, mas para isso é fundamental garantir a protecção/segurança das mesmas. Face a complexidade das organizações e do aperfeiçoamento cada vez maior das formas de ataque a um sistema informático, garantir a segurança não é tarefa fácil.

Para verificar se existem práticas de segurança adequadas e se os procedimentos adoptados estão em conformidade com a política de segurança, são feitas periodicamente avaliações com recurso a auditoria de segurança. Esta deve ser um recurso complementar no processo

de segurança e, apesar de ser uma prática adoptada na sua grande parte apenas por grandes organizações, ela poderá ser também praticada por organizações de qualquer dimensão, pois desta forma, estando a informação protegida, ela pode ser utilizada como uma vantagem estratégica, agregando valor para a organização.

Bibliografia

Amado, João, (2006), *Hackers - técnicas de defesa e ataque*. (3ª Ed.), Lisboa/Porto/Coimbra: FCA – Editora de Informática, Lda.

Carneiro, Alberto. (2009). *Auditoria e Controlo de Sistemas de Informação*. Lisboa/Porto/Coimbra: FCA – Editora de Informática, Lda.

Carneiro, Alberto. (2004). (2ª Ed.). *Auditoria de Sistemas de Informação*. Lisboa/Porto/Coimbra: FCA – Editora de Informática, Lda.

Carneiro, Alberto. (2002). *Introdução à Segurança dos Sistemas de Informação*. Lisboa/Porto/Coimbra: FCA – Editora de Informática, Lda.

Dantas, Jorge. (2010). "Conceitos e Organização da Auditoria: Planejamento e Execução", disponível em http://www.slideshare.net/jorgedantas/auditoria-2, [consultado a 23/09/09].

Downing, Douglas e Covington, Michael e Covington, Melody Maudin. (2001). *Dicionário de termos informáticos e da internet*. Lisboa: Paralelo Editora, Lda.

Fegundes, Eduardo Mayer. (2004) "COBIT: um kit de ferramentas para a excelência na gestão de TI", disponível em http://www.cepromat.mt.gov.br/arquivos/A_5e375755312b3345b521def9a5474c66cobit.pdf, [consultado a 03/08/11].

Ferreira, Jorge e Alves, Sebastião. (1995). *Manual Técnico de Segurança dos Sistemas e Tecnologias de Informação*. Instituto de Informática

Ferreira, Daniele *et al*. (2001). "Proposta para uma Política de Segurança de Dados aplicada às Secretarias de Receita", disponível em http://www.scribd.com/doc/6841289/298Redes, [consultado a 03/08/11].

Gil, António de Loureiro. (1999). (4ª Ed.) *Auditoria de computadores*. São Paulo: Atlas

Il Tec. (1993). *Dicionário de Termos informáticos*. Lisboa: Edições Cosmo

ISACA, "Cobit", disponível em http://www.isaca.org [consultado a 22/08/11]

Mamede, Henrique São. (2006). *Segurança Informática nas Organizações*. Lisboa/Porto/Coimbra: FCA – Editora de Informática, Lda.

Medeiros, Carlos Diego Russo. (2001) "Segurança da informação – implantação de medidas e ferramentas de segurança da informação", disponível em http://www.linuxsecurity.com.br/info/general/TCE_Seguranca_da_Informacao.pdf, [consultado a 03/08/11].

Michel, Maria Helena (2005). *Metodologia e Pesquisa Cientifica em Ciências Sociais: um guia prático para acompanhamento da disciplina e elaboração de trabalhos monográficos*. São Paulo: Atlas S.A.

Monteiro, Edmundo e Boavida, Fernando. (2000). (5ª Ed.) *Engenharia de redes informáticas*. Lisboa/Porto/Coimbra: FCA – Editora de Informática, Lda.

Neto, Abílio Bueno e Solonca, Davi (2007) "Auditoria de sistemas informatizados", disponível em http://busca.unisul.br/pdf/88277_Abilio.pdf, [consultado a 03/08/11].

Oliveira, Wilson. (2000). *Técnicas para Hackers - soluções para segurança*. Lisboa: Centro Atlântico

Pedro, José Maria (2005), "Segurança informática em auditoria" disponível em http://knowkapital.eu/extra/artigos/Seg_e_Auditoria_IGF.pdf, [consultado a 03/08/11].

Pinheiro, José Maurício dos Santos (2007) "Os Benefícios da Politica de Segurança baseada na Avaliação de Riscos e na Integração de Ferramentas", disponível em http://www.foa.org.br/cadernos/edicao/04/28.pdf, [consultado a 03/08/11].

Rego, Antônio Marcos Passos de Sousa et al (s.d.) "A utilização de C.O.S.O. na contralodoria: um estudo no Brasil", disponível em http://www.intercostos.org/documentos/Passos.pdf, [consultado a 03/08/11].

Silva, Miguel Mira da e Silva, Alberto e Romão, Artur e Conde, Nuno (2003). (2ª Ed.) *Comercio Electrónico na Internet*. Lisboa/Porto/Coimbra: LIDEL – Edições Técnicas Lda.

Silva, Pedro Tavares e Carvalho, Hugo e Torres, Catarina Botelho. (2003). *Segurança dos Sistemas de Informação – Gestão Estratégica de Segurança Empresarial*. Lisboa: Centro Atlântico

Silva, Valflávio Bernardes (2005). "Impacto na Implementação de Política de Segurança da Informação na Novo Nordisk produção Farmacêutica do Brasil", disponível em http://www.ccet.unimontes.br/arquivos/monografias/76.pdf, [consultado a 03/08/11].

Simões, Jorge (2004). "Segurança de Sistemas Informáticos", disponível em http://paginas.ispgaya.pt/~jsimoes/src/seguranca.pdf, [consultado a 03/08/11].

Spanceski, Francini Reitz (2004), "Politica de segurança da informação – Desenvolvimento de um modelo voltado para instituições de ensino", disponível em http://www.mlaureano.org/aulas_material/orientacoes2/ist_2004_francini_politicas.pdf , [consultado a 03/08/11].

Zúquete, André. (2006). *Segurança em redes informáticas*. Lisboa/Porto/Coimbra: FCA – Editora de Informática, Lda.

Zúquete, André. (2008). (2ª Ed.) *Segurança em redes informáticas*. Lisboa: FCA – Editora de Informática, Lda.

A Anexo

A.1 Checklist, segurança informática das escolas secundárias

Este anexo, representa a *checklist*, contendo uma série de questões relevantes sobre segurança e teve como objectivo recolher as informações necessárias para conhecer e analisar as práticas de segurança informática das escolas secundárias da cidade da Praia. Esta *checklist* compõe-se de 44 itens, sendo alguns desses itens constituídos por 2-4 sub-itens. Para uma melhor analise destas questões sobre a segurança, interrogou-se sobre a infra-estrutura tecnológica das escolas, representada no ponto seguinte.

Questões/Descrição	Resposta	
	Sim	Não
Segurança Física		
Existem mecanismos de controlo de acesso à organização		
Existem mecanismos de controlo de acesso dentro da organização (particularmente nos lugares onde estão os equipamentos críticos)		
Estão definidos os requisitos de segurança para a localização dos equipamentos críticos (calor, humidade)		
Existe monitorização das condições ambientais para todos os equipamentos da organização (proteger os equipamentos do calor, humidade, poeira)		
Os bastidores estão localizados fora de acesso público		
Os outros equipamentos estão localizados em locais seguros		
Há um controlo adicional de segurança nos locais onde estão os equipamentos críticos (controlos que possam minimizar os riscos tais como roubo, inundação, incêndio)		
São efectuados testes nos equipamentos de emergência regularmente		
Existem geradores e sistemas UPS para equipamentos críticos		
O cabeamento encontra-se estruturado		
Existe stock de equipamentos		

Existem equipamentos para casos de emergência (protecção contra incêndio como extintores, detecção de fumaça)		
A manutenção dos equipamentos é feita por técnicos especializados		
Existem formas de registar as falhas dos equipamentos		
Existe um centro Help Desck		
Segurança Lógica		
Existem exigências definidas e documentadas de controlo de acesso lógico:		
- restrições e permissões de acesso e a serviços;		
- utilização segura de *password*.		
Existem requisitos de segurança para a utilização de sistemas novos		
Existem oportunidades de teste isolado dos procedimentos operacionais		
Os softwares utilizados são licenciados		
Existe proibição para a utilização de software desautorizado		
Existem auditorias internas para averiguar aspectos relevantes tais como a utilização de software não autorizado		
Os sistemas utilizados são sujeitos a actualizações (com frequência)		
Existe um sistema antivírus actualizado e centralizado		
Realizam regularmente cópias de segurança		
Existem especificações explícitas para o efeito (o quê/quando/como/quem)		
Existem política de segurança de controlo de acesso a rede		
Os documentos da rede estão devidamente identificados e documentados (nome, endereço, localização e usuário dos computadores)		
Existe algum controlo para proteger a integridade no processamento dos dados		
Estão definidos os requisitos para a utilização da Internet		
Existe um firewall ou um servidor proxy para ditar as permissões e restrições (conteúdos a serem acedidos pela internet)		
São efectuadas as actualizações para a lista negra (os sites e conteúdos		

que não podem ser acedidos)		
Existe alguma protecção nas aplicações para impedir o acesso não autorizado às mesmas		
Segurança Recursos Humanos		
Existem programas de formação/sensibilização relacionadas com questões de segurança		
Existe treinamento em segurança (alguma campanha de sensibilização)		
Existem políticas de segurança definidas para: ▪ utilização de password;		
▪ manuseio/utilização dos equipamentos;		
▪ Controlo de acesso;		
▪ definição de responsabilidades.		
Existe uma definição clara das funções e responsabilidades individuais de cada funcionário		
São informados das regras e princípios vigentes na organização		
São cessadas todas as permissões quando um funcionário abandona a organização		
São especificados os requisitos para recrutamento de novos funcionários		
Planos e Politica de segurança		
Existem planos de segurança para situações de emergência		
Existe uma política de segurança (praticável e eficaz) aprovada pela gerência, publicada e comunicada a todos os funcionários		
Esta Politica é sujeita a revisões periódicas de acordo com as mudanças que ocorrem na organização		

A.1.1 Infra-estrutura tecnológica das escolas

Infra-estrutura das TIC	
Número de computadores/estação de trabalho	
Número de servidores	
Número de router	
Número de switch	
Número de hub	
Número de impressoras	
Número de gerador	
Número de UPS	
Demais equipamentos informáticos	
Número de utilizadores das TIC	
As funções suportadas pelas TIC	
Número de técnicos especializados na área das TIC	
Nível hierárquico do responsável pela área das TIC	
Existe ligação Internet ao sistema informático da escola	